



Cisco FXOS トラブルシューティングガイド（**Threat Defense** を実行している **Cisco Firepower 1000/2100** および **Cisco Secure Firewall 1200/3100/4200** 向け）

最終更新：2025 年 4 月 8 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	Firepower 1000/2100、Cisco Secure Firewall 1200/3100/4200 セキュリティアプライアンス CLI について 1
	FXOS CLI の階層 2
	CLI に関するオンラインヘルプ 3
第 2 章	グローバル FXOS CLI コマンド 5
	グローバル FXOS CLI コマンド 5
第 3 章	FXOS CLI のトラブルシューティング コマンド 7
	FXOS CLI シャーシ モードトラブルシューティング コマンド 7
	FXOS CLI イーサネット アップリンク モードトラブルシューティング コマンド 12
	FXOS CLI ファブリック インターコネクト モードトラブルシューティング コマンド 15
	Cisco Secure Firewall 3100 の connect local-mgmt トラブルシューティング コマンド 19
	アプライアンスモードでの Cisco Secure Firepower 4200 の connect local-mgmt トラブルシューティング コマンド 31
	FXOS CLI セキュリティ サービス モードトラブルシューティング コマンド 40
	Cisco Secure Firewall 1200/3100/4200 CLI モニタリングモードのトラブルシューティング コマンド 42
	Cisco Secure Firewall 3100/4200 のパケットキャプチャ 42
	パケット キャプチャの注意事項および制限事項 43
	パケット キャプチャ セッションの作成または編集 43
	パケット キャプチャ セッションの削除 47
第 4 章	イメージ管理 49

ディザスタリカバリの概要	49
ベース インストール ソフトウェア バージョンを使用したシステムの再イメージ化	50
ROMMON からの工場出荷時設定へのリセットの実行（パスワードのリセット）	53
新しいソフトウェアバージョンを使用したシステムの再イメージ化	55
マルチインスタンスモードのパッケージのダウンロード	59
SSD ファイルシステムの再フォーマット（Firepower 2100）	60
ROMMON からの起動	60
完全な再イメージ化の実行	68
管理者パスワードの変更	73
Threat Defense がオフラインの場合の管理者パスワードの変更	74
クラウドからの登録解除	75
Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 FXOS トラブルシューティングの履歴	77



第 1 章

Firepower 1000/2100、Cisco Secure Firewall 1200/3100/4200 セキュリティアプライアンス CLI について

このトラブルシューティングガイドでは、Firepower 1000、Firepower 2100、Cisco Secure Firewall 1200、Cisco Secure Firewall 3100、および Cisco Secure Firewall 4200 セキュリティアプライアンスシリーズの Firepower eXtensible オペレーティングシステム（FXOS）コマンドラインインターフェイス（CLI）について説明します。



(注) SSH クライアント管理ポートの CLI は Secure Firewall Threat Defense にデフォルト設定されます。FXOS CLI にアクセスするには、**connect fxos** コマンドを使用します。

Firepower 1000/2100、Cisco Secure Firewall 1200、Cisco Secure Firewall 3100、Cisco Secure Firewall 4200 コンソールポートでは、FXOS CLI プロンプトがデフォルトの CLI になります。Threat Defense CLI には、**connect ftd** コマンドを使用してアクセスできます。

FXOS CLI にログインすると、以下で説明するコマンドを使用して、Firepower 1000、Firepower 2100、Cisco Secure Firewall 1200、Cisco Secure Firewall 3100、Cisco Secure Firewall 4200 シリーズデバイスの FXOS プラットフォームを表示してトラブルシューティングできます。

Firepower 1000/2100、Cisco Secure Firewall 1200、Cisco Secure Firewall 3100、または Cisco Secure Firewall 4200 デバイスに Threat Defense がインストールされている場合、FXOS CLI では設定を変更できません。FXOS CLI で設定の変更を試みると、**commit-buffer** コマンドによりエラーが返されます。

Threat Defense CLI の詳細については、[Threat Defense のコマンドリファレンス](#)を参照してください。

- [FXOS CLI の階層（2 ページ）](#)
- [CLI に関するオンラインヘルプ（3 ページ）](#)

FXOS CLI の階層

FXOS CLI のコマンドモードは階層構造になっており、EXEC モードが階層の最上位となります。高いレベルのモードは、低いレベルのモードに分岐します。高いレベルのモードから 1 つ低いレベルのモードに移動するには、**create**、**enter**、および **scope** コマンドを使用します。また、モード階層で 1 つ高いレベルに移動するには、**exit** コマンドを使用します。また、モード階層の最上位に移動するには **top** コマンドも使用できます。

各モードには、そのモードで入力できるコマンドのセットが含まれています。各モードで使用できるコマンドの大部分は、関連する管理対象オブジェクトに関連しています。

各モードの CLI プロンプトには、モード階層における現在のモードのフルパスが表示されます。これにより、コマンドモード階層内での現在位置を容易に判断できます。また、この機能は階層内を移動する際にも非常に役立ちます。

次の表は、主要なコマンドモード、各モードへのアクセスに使用するコマンド、および各モードに関連する CLI プロンプトを示しています。

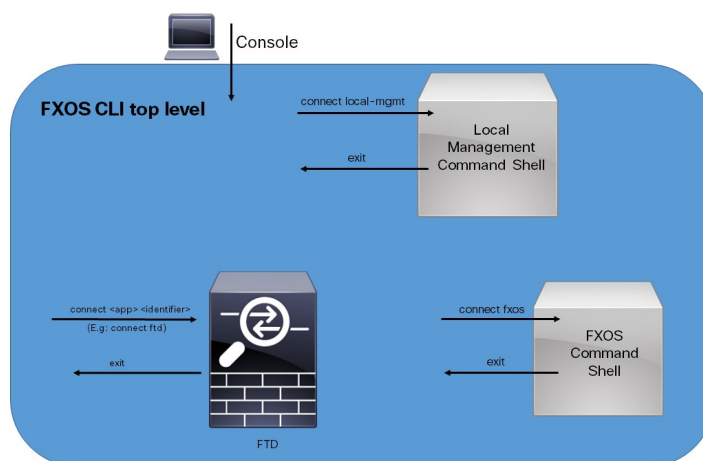
表 1: 主要なコマンドモードとプロンプト

モード名	アクセスに使用するコマンド	モードプロンプト
EXEC	任意のモードで top コマンド	#
シャーシ	EXEC モードから scope chassis コマンド	/chassis #
イーサネット アップリンク	EXEC モードで scope eth-uplink コマンド	/eth-uplink #
ファブリック インターコネクト	EXEC モードから scope fabric-interconnect コマンド	/fabric-interconnect #
ファームウェア	EXEC モードから scope firmware コマンド	/firmware #
モニタリング	EXEC モードから scope monitoring コマンド	/monitoring #
組織	EXEC モードから scope org コマンド	/org #
セキュリティ	EXEC モードから scope security コマンド	/security #
サーバ	EXEC モードから scope server コマンド	/server #

モード名	アクセスに使用するコマンド	モード プロンプト
ssa	EXEC モードから scope ssa コマンド	/ssa #
システム	EXEC モードから scope system コマンド	/system #

次の図は、FXOS CLI のトップレベルから FXOS コマンドシェル、ローカル管理コマンドシェル、および Firepower Threat Defense CLI にアクセスするために実行できるコマンドの概要を示したものです。コンソールアクセスが必要であることを注意してください。

図 1: Firepower 1000/2100 および Cisco Secure Firewall 3100 FXOS CLI 接続図



CLI に関するオンラインヘルプ

いつでも ? 文字を入力して、その時点のコマンド構文の状態に応じた使用可能なオプションを表示できます。

プロンプトに何も入力せずに ? を入力すると、現在のモードで使用できるコマンドがすべて表示されます。コマンドの一部を入力して ? を入力すると、その時点のコマンド構文内の位置で使用可能なキーワードと引数がすべて表示されます。



第 2 章

グローバル FXOS CLI コマンド

・ [グローバル FXOS CLI コマンド \(5 ページ\)](#)

グローバル FXOS CLI コマンド

以下のコマンドは、FXOS CLI のすべてのモードにグローバルに対応します。

コマンド	説明
acknowledge fault	エラーを確認します。コマンドの構文： 次に例を示します。 <code>acknowledge fault 1</code> <i>id</i> はエラー識別番号です。有効な値の範囲は 0 ～ 9223372036854775807 です。
clear	管理対象オブジェクトをクリアします。
commit-buffer	トランザクションバッファをコミットします。
connect	別の CLI に接続します。 次に例を示します。 <code>connect ftd</code>

コマンド	説明
connect fxos [admin]	[admin] キーワードを使用すると、ユーザーが追加のコマンドを実行できる特権モードで FXOS に接続できます。 たとえば、Firepower eXtensible Operating System (FXOS) show-tech ファイルを生成するには、次のようにします。 <pre>firewall# connect fxos admin Configuring session. . Connecting to FXOS. 1 firepower-3140# connect local-mgmt Warning: network service is not available when entering 'connect local-mgmt' firepower-3140(local-mgmt)# show tech-support fprm <CR> > Redirect it to a file >> Redirect it to a file in append mode brief Brief detail Detail Pipe command output to filter </pre> </pre>
discard-buffer	トランザクションバッファを破棄します。
end	EXEC モードに入ります。
exit	コマンドインタプリタを終了します。
scope	新しいモードを開始します。
set	プロパティの値を設定します。
show	システム情報を表示します。
terminal	端末
top	モードの最上位に移動します。
ucspe-copy	UCSPE にファイルをコピーします。
up	1 つ上位のモードに移動します。
where	現在のモードに関する情報を表示します。
backup	バックアップします。



第 3 章

FXOS CLI のトラブルシューティング コマンド

- [FXOS CLI シャーシモードトラブルシューティング コマンド \(7 ページ\)](#)
- [FXOS CLI イーサネットアップリンク モードトラブルシューティング コマンド \(12 ページ\)](#)
- [FXOS CLI ファブリック インターコネクト モードトラブルシューティング コマンド \(15 ページ\)](#)
- [Cisco Secure Firewall 3100 の connect local-mgmt トラブルシューティング コマンド \(19 ページ\)](#)
- [アプライアンスモードでの Cisco Secure Firepower 4200 の connect local-mgmt トラブルシューティング コマンド \(31 ページ\)](#)
- [FXOS CLI セキュリティ サービス モードトラブルシューティング コマンド \(40 ページ\)](#)
- [Cisco Secure Firewall 1200/3100/4200 CLI モニタリングモードのトラブルシューティング コマンド \(42 ページ\)](#)
- [Cisco Secure Firewall 3100/4200 のパケットキャプチャ \(42 ページ\)](#)

FXOS CLI シャーシモードトラブルシューティング コマンド

システムに関する問題をトラブルシューティングするには、以下のシャーシモード FXOS CLI コマンドを使用します。

show environment

シャーシの環境情報を表示します。

次に例を示します。

```
FPR2100 /chassis # show environment expand detail
Chassis 1:
Overall Status: Power Problem
Operability: Operable
Power State: Ok
Thermal Status: Ok
PSU 1:
```

```

Overall Status: Powered Off
Operability: Unknown
Power State: Off
Voltage Status: Unknown
PSU 2:
Overall Status: Operable
Operability: Operable
Power State: On
Voltage Status: Ok
Tray 1 Module 1:
Overall Status: Operable
Operability: Operable
Power State: On
Fan 1:
Overall Status: Operable
Operability: Operable
Power State: On
Fan 2:
Overall Status: Operable
Operability: Operable
Power State: On
Fan 3:
Overall Status: Operable
Operability: Operable
Power State: On
Fan 4:
Overall Status: Operable
Operability: Operable
Power State: On
Server 1:
Overall Status: Ok
Memory Array 1:
Current Capacity (MB): 32768
Populated: 2
DIMMs:
ID Overall Status Capacity (MB)
---
1 Operable 16384
2 Operable 16384
CPU 1:
Presence: Equipped
Cores: 8
Product Name: Intel(R) Xeon(R) CPU D-1548 @ 2.00GHz
Vendor: GenuineIntel
Thermal Status: OK
Overall Status: Operable
Operability: Operable

```



(注) Cisco Secure Firewall 3100 デバイスでデュアルファンモジュールを取り外す際に、ファンの実際のステータスを表示するには、**show environment basic** および **show environment expand** コマンドを使用します。

show environmentbasic

シャーシおよび CPU の温度データを表示します。
次に例を示します。

```

FPR2100 /chassis # show environment basic
***** Chassis Temps *****
Inlet temperature is 75 degrees Celsius

```

```
***** CPU Data *****
Core Temperature 0 is 93 degrees Celsius
Core Temperature 1 is 93 degrees Celsius
Core Temperature 2 is 94 degrees Celsius
Core Temperature 3 is 92 degrees Celsius
```

scope fan

Firepower 2110、2120、Cisco Secure Firewall 3100、および Cisco Secure Firewall 4200 デバイスでファンモードを開始します。

scope fan-module

Firepower 2130、2140、Cisco Secure Firewall 3100、および Cisco Secure Firewall 4200 デバイスでファンモードを開始します。このモードでは、シャーシファンに関する詳細情報を表示できます。

次に例を示します。

```
FPR2100 /chassis # show fan-module expand detail
Fan Module:
  Tray: 1
  Module: 1
  Overall Status: Operable
  Operability: Operable
  Power State: On
  Presence: Equipped
  Product Name: Cisco Firepower 2000 Series Fan Tray
  PID: FPR2K-FAN
  Vendor: Cisco Systems, Inc
  Fan:
    ID: 1
    Overall Status: Operable
    Operability: Operable
    Power State: On
    Presence: Equipped
    ID: 2
    Overall Status: Operable
    Operability: Operable
    Power State: On
    Presence: Equipped
```

show inventory

シャーシ番号、ベンダー、シリアル番号などのインベントリ情報を表示します。

注：このコマンドは、Firepower 2130、Cisco Secure Firewall 3100 および 4200 デバイスにのみ適用されます。

次に例を示します。

```
FPR2100 /chassis # show inventory
Chassis  PID          Vendor          Serial (SN) HW Revision
-----  -
1 FPR-2140      Cisco Systems, In JAD201005FC 0.1
```

show inventory expand

FRU 対応コンポーネント（シャーシ、PSU、ネットワーク モジュールなど）に関する詳細なインベントリ情報を表示します。

次に例を示します。

```
FPR2100 /chassis # show inventory expand detail
Chassis 1:
  Product Name: Cisco Firepower 2000 Appliance
  PID: FPR-2130
```

```

VID: V01
Vendor: Cisco Systems, Inc
Model: FPR-2130
Serial (SN): JAD2012091X
HW Revision: 0.1
PSU 1:
  Presence: Equipped
  Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
  PID: FPR2K-PWR-AC-400
  VID: V01
  Vendor: Cisco Systems, Inc
  Serial (SN): LIT2010CAFE
  HW Revision: 0
PSU 2:
  Presence: Equipped
  Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
  PID: FPR2K-PWR-AC-400
  VID: V01
  Vendor: Cisco Systems, Inc
  Serial (SN): LIT2010CAFE
  HW Revision: 0
Fan Modules:
  Tray 1 Module 1:
    Presence: Equipped
    Product Name: Cisco Firepower 2000 Series Fan Tray
    PID: FPR2K-FAN
    Vendor: Cisco Systems, Inc
Fans:
  ID Presence
  --
  1 Equipped
  2 Equipped
  3 Equipped
  4 Equipped
Fabric Card 1:
  Description: Cisco SSP FPR 2130 Base Module
  Number of Ports: 16
  State: Online
  Vendor: Cisco Systems, Inc.
  Model: FPR-2130
  HW Revision: 0
  Serial (SN): JAD2012091X
  Perf: N/A
  Operability: Operable
  Overall Status: Operable
  Power State: Online
  Presence: Equipped
  Thermal Status: N/A
  Voltage Status: N/A
Fabric Card 2:
  Description: 8-port 10 Gigabit Ethernet Expansion Module
  Number of Ports: 8
  State: Online
  Vendor: Cisco Systems, Inc.
  Model: FPR-NM-8X10G
  HW Revision: 0
  Serial (SN): JAD19510AKD
  Perf: N/A
  Operability: Operable
  Overall Status: Operable
  Power State: Online
  Presence: Equipped
  Thermal Status: N/A
  Voltage Status: N/A

```

scope psu

電源ユニットモードを開始します。このモードでは、電源ユニットに関する詳細情報を表示できます。

次に例を示します。

```
FPR2100 /chassis # show psu expand detail
PSU:
  PSU: 1
  Overall Status: Powered Off
  Operability: Unknown
  Power State: Off
  Presence: Equipped
  Voltage Status: Unknown
  Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
  PID: FPR2K-PWR-AC-400
  VID: V01
  Vendor: Cisco Systems, Inc
  Serial (SN): LIT2010CAFE
  Type: AC
  Fan Status: Ok
  PSU: 2
  Overall Status: Operable
  Operability: Operable
  Power State: On
  Presence: Equipped
  Voltage Status: Ok
  Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
  PID: FPR2K-PWR-AC-400
  VID: V01
  Vendor: Cisco Systems, Inc
  Serial (SN): LIT2010CAFE
  Type: AC
  Fan Status: Ok
```

scope stats

統計情報モードを開始します。このモードでは、シャーシに関する詳細な統計情報を表示できます。

次に例を示します。

```
FPR2100 /chassis # show stats
Chassis Stats:
  Time Collected: 2016-11-14T21:19:46.317
  Monitored Object: sys/chassis-1/stats
  Suspect: No
  Outlet Temp1 (C): 43.000000
  Outlet Temp2 (C): 41.000000
  Inlet Temp (C): 30.000000
  Internal Temp (C): 34.000000
  Thresholded: 0
Fan Stats:
  Time Collected: 2016-11-14T21:19:46.317
  Monitored Object: sys/chassis-1/fan-module-1-1/fan-1/stats
  Suspect: No
  Speed (RPM): 17280
  Thresholded: 0
  Time Collected: 2016-11-14T21:19:46.317
  Monitored Object: sys/chassis-1/fan-module-1-1/fan-2/stats
  Suspect: No
  Speed (RPM): 17340
  Thresholded: 0
  Time Collected: 2016-11-14T21:19:46.317
  Monitored Object: sys/chassis-1/fan-module-1-1/fan-3/stats
```

```

Suspect: No
Speed (RPM): 17280
Thresholded: 0
Time Collected: 2016-11-14T21:19:46.317
Monitored Object: sys/chassis-1/fan-module-1-1/fan-4/stats
Suspect: No
Speed (RPM): 17280
Thresholded: 0
Psu Stats:
Time Collected: 2016-11-14T21:19:46.318
Monitored Object: sys/chassis-1/psu-1/stats
Suspect: No
Input Current (A): 0.000000
Input Power (W): 8.000000
Input Voltage (V): 0.000000
Psu Temp1 (C): 32.000000
Psu Temp2 (C): 36.000000
Psu Temp3 (C): 32.000000
Fan Speed (RPM): 0
Thresholded: 0
Time Collected: 2016-11-14T21:19:46.318
Monitored Object: sys/chassis-1/psu-2/stats
Suspect: No
Input Current (A): 0.374000
Input Power (W): 112.000000
Input Voltage (V): 238.503006
Psu Temp1 (C): 36.000000
Psu Temp2 (C): 47.000000
Psu Temp3 (C): 47.000000
Fan Speed (RPM): 2240
Thresholded: 0
CPU Env Stats:
Time Collected: 2016-11-14T21:19:46.317
Monitored Object: sys/chassis-1/blade-1/board/cpu-1/env-stats
Suspect: No
Temperature (C): 46.000000
Thresholded: 0
Time Collected: 2016-11-14T21:19:46.317
Monitored Object: sys/chassis-1/blade-1/npu/cpu-1/env-stats
Suspect: No
Temperature (C): 38.000000
Thresholded: 0

```

FXOS CLI イーサネット アップリンク モードトラブルシューティング コマンド

システムに関する問題をトラブルシューティングするには、以下のイーサネットアップリンクモード FXOS CLI コマンドを使用します。

show detail

Firepower 1000/2100、Cisco Secure Firewall 3100、または Cisco Secure Firewall 4200 デバイスのイーサネットアップリンクに関する詳細情報を表示します。

次に例を示します。

```

FPR2100 /eth-uplink # show detail
Ethernet Uplink:
Mode: Security Node

```



```
MAC Table Aging Time (dd:hh:mm:ss): 00:04:01:40
VLAN Port Count Optimization: Disabled
Current Task:
```

scope fabric a

イーサネットアップリンク インターフェイス モードを開始します。このモードでは、ポートチャンネル、統計、インターフェイスに関する情報を表示できます。
次に例を示します。

```
FPR2100 /eth-uplink/fabric # show interface
```

Interface:

Port Name	Port Type	Admin State	Oper State	State Reason
Ethernet1/1	Data	Enabled	Up	Up
Ethernet1/2	Data	Enabled	Link Down	Down
Ethernet1/3	Data	Disabled	Link Down	Down
Ethernet1/4	Data	Disabled	Link Down	Down
Ethernet1/5	Data	Disabled	Link Down	Down
Ethernet1/6	Data	Disabled	Link Down	Down
Ethernet1/7	Data	Disabled	Link Down	Down
Ethernet1/8	Data	Disabled	Link Down	Down
Ethernet1/9	Data	Disabled	Link Down	Down
Ethernet1/10	Data	Disabled	Link Down	Down
Ethernet1/11	Data	Disabled	Link Down	Down
Ethernet1/12	Data	Disabled	Link Down	Down
Ethernet1/13	Data	Disabled	Link Down	Down
Ethernet1/14	Data	Disabled	Link Down	Down
Ethernet1/15	Data	Disabled	Link Down	Down
Ethernet1/16	Data	Disabled	Link Down	Down
Ethernet2/1	Data	Disabled	Link Down	Down
Ethernet2/2	Data	Disabled	Link Down	Down
Ethernet2/3	Data	Disabled	Link Down	Down
Ethernet2/4	Data	Disabled	Link Down	Down
Ethernet2/5	Data	Disabled	Link Down	Down
Ethernet2/6	Data	Disabled	Link Down	Down
Ethernet2/7	Data	Disabled	Link Down	Down
Ethernet2/8	Data	Disabled	Link Down	Down

```
FPR2100 /eth-uplink/fabric # show port-channel
```

Port Channel:

Port Channel Id	Name	Port Type	Admin State
Oper State	State Reason		
1	Port-channel1	Data	Disabled
Link Down		Down	

```
FPR2100 /eth-uplink/fabric/port-channel # show stats
```

Ether Error Stats:

```
Time Collected: 2016-11-14T21:27:16.386
Monitored Object: fabric/lan/A/pc-1/err-stats
Suspect: No
Rcv (errors): 0
Align (errors): 0
Fcs (errors): 0
Xmit (errors): 0
Under Size (errors): 0
Out Discard (errors): 0
Deferred Tx (errors): 0
Int Mac Tx (errors): 0
Int Mac Rx (errors): 0
Thresholded: Xmit Delta Min
```

Ether Loss Stats:

```
Time Collected: 2016-11-14T21:27:16.386
```

```

Monitored Object: fabric/lan/A/pc-1/loss-stats
Suspect: No
Single Collision (errors): 0
Multi Collision (errors): 0
Late Collision (errors): 0
Excess Collision (errors): 0
Carrier Sense (errors): 0
Giants (errors): 0
Symbol (errors): 0
SQE Test (errors): 0
Thresholded: 0
Ether Pause Stats:
Time Collected: 2016-11-14T21:27:16.386
Monitored Object: fabric/lan/A/pc-1/pause-stats
Suspect: No
Recv Pause (pause): 0
Xmit Pause (pause): 0
Resets (resets): 0
Thresholded: 0
Ether Rx Stats:
Time Collected: 2016-11-14T21:27:16.386
Monitored Object: fabric/lan/A/pc-1/rx-stats
Suspect: No
Total Packets (packets): 0
Unicast Packets (packets): 0
Multicast Packets (packets): 0
Broadcast Packets (packets): 0
Total Bytes (bytes): 0
Jumbo Packets (packets): 0
Thresholded: 0
Ether Tx Stats:
Time Collected: 2016-11-14T21:27:16.386
Monitored Object: fabric/lan/A/pc-1/tx-stats
Suspect: No
Total Packets (packets): 0
Unicast Packets (packets): 0
Multicast Packets (packets): 0
Broadcast Packets (packets): 0
Total Bytes (bytes): 0
Jumbo Packets (packets): 0
FPR2100 /eth-uplink/fabric/interface # show stats
Ether Error Stats:
Time Collected: 2016-11-14T21:27:46.395
Monitored Object: sys/switch-A/slot-1/switch-ether/port-1/err-stats
Suspect: No
Rcv (errors): 0
Align (errors): 0
Fcs (errors): 0
Xmit (errors): 0
Under Size (errors): 0
Out Discard (errors): 0
Deferred Tx (errors): 0
Int Mac Tx (errors): 0
Int Mac Rx (errors): 0
Thresholded: Xmit Delta Min
Ether Loss Stats:
Time Collected: 2016-11-14T21:27:46.395
Monitored Object: sys/switch-A/slot-1/switch-ether/port-1/loss-stats
Suspect: No
Single Collision (errors): 0
Multi Collision (errors): 0
Late Collision (errors): 0
Excess Collision (errors): 0
Carrier Sense (errors): 0

```

```

Giants (errors): 7180
Symbol (errors): 0
SQE Test (errors): 0
Thresholded: 0
Ether Pause Stats:
Time Collected: 2016-11-14T21:27:46.395
Monitored Object: sys/switch-A/slot-1/switch-ether/port-1/pause-stats
Suspect: No
Recv Pause (pause): 0
Xmit Pause (pause): 0
Resets (resets): 0
Thresholded: 0
Ether Rx Stats:
Time Collected: 2016-11-14T21:27:46.395
Monitored Object: sys/switch-A/slot-1/switch-ether/port-1/rx-stats
Suspect: No
Total Packets (packets): 604527
Unicast Packets (packets): 142906
Multicast Packets (packets): 339031
Broadcast Packets (packets): 122590
Total Bytes (bytes): 59805045
Jumbo Packets (packets): 0
Thresholded: 0
Ether Tx Stats:
Time Collected: 2016-11-14T21:27:46.395
Monitored Object: sys/switch-A/slot-1/switch-ether/port-1/tx-stats
Suspect: No
Total Packets (packets): 145018
Unicast Packets (packets): 145005
Multicast Packets (packets): 0
Broadcast Packets (packets): 13
Total Bytes (bytes): 13442404
Jumbo Packets (packets): 0
Thresholded: 0

```

FXOS CLI ファブリック インターコネクト モード トラブルシューティング コマンド

システムに関する問題をトラブルシューティングするには、以下のファブリック インターコネクト モード FXOS CLI コマンドを使用します。

show card

ファブリック カードに関する情報を表示します。
次に例を示します。

```

FPR2100 /fabric-interconnect # show card detail expand
Fabric Card:
  Id: 1
  Description: Cisco SSP FPR 2130 Base Module
  Number of Ports: 16
  State: Online
  Vendor: Cisco Systems, Inc.
  Model: FPR-2130
  HW Revision: 0
  Serial (SN): JAD2012091X
  Perf: N/A
  Operability: Operable
  Overall Status: Operable

```

```

Power State: Online
Presence: Equipped
Thermal Status: N/A
Voltage Status: N/A

```

show card

ファブリックカードに関する詳細情報を表示します。このコマンドを使用すると、ネットワークモジュールの詳細を表示できます。
次に例を示します。

```
# firepower-4225 /fabric-interconnect # show card detail expand
```

```

Fabric Card:
Id: 2
Description: 2-port 100 Gigabit Ethernet Expansion Module
Number of Ports: 2
Admin State: Enabled
State: Online
Vendor: Cisco Systems, Inc.
Model: FPR-X-NM-2X100G
Serial (SN): FJZ26390V7D
Perf: N/A
Operability: Operable
Overall Status: Online
Power State: Online
Presence: Equipped
Thermal Status: N/A
Voltage Status: N/A
Current Task:

```

show image

使用可能なイメージをすべて表示します。

```
firepower /firmware # show image
```

Name	Type	Version
cisco-ftd.6.2.0.131.csp	Firepower Cspapp	6.2.0.131
cisco-ftd.6.2.0.140.csp	Firepower Cspapp	6.2.0.140
cisco-ftd.6.2.0.175.csp	Firepower Cspapp	6.2.0.175
fxos-k8-fp2k-firmware.0.4.04.SPA	Firepower Firmware	0.4.04
fxos-k8-fp2k-lfbff.82.1.1.303i.SSA	Firepower System	82.1(1.303i)
fxos-k8-fp2k-npu.82.1.1.303i.SSA	Firepower Npu	82.1(1.303i)
fxos-k8-fp2k-npu.82.1.1.307i.SSA	Firepower Npu	82.1(1.307i)
fxos-k9-fp2k-manager.82.1.1.303i.SSA	Firepower Manager	82.1(1.303i)

show inventory expand

ファブリックカードに関する詳細情報をすべて表示します。このコマンドを使用すると、ネットワークモジュールの詳細を表示できます。

```
firepower-4225 /fabric-interconnect # show inventory expand
A:
```

```
Fabric Card:
```

Slot	Description	Num Ports	State	PID	Serial (SN)
0	Logical Slot for Management Interface	2	N/A	FPR-4225	FJZ26345ZGZ
1	Cisco FPR 4225 Base Module	8	On	FPR-4225	FJZ26345ZGZ
3	4-port 200 Gigabit Ethernet Expansion Module				

4 Online

FPR-X-NM-4X200G FJZ25430132

show package

使用可能なパッケージをすべて表示します。

```
firepower /firmware # show package
Name                                     Package-Vers
-----
cisco-ftd-fp2k.6.2.0.131-303i.SSA      6.2(0.131-303i)
cisco-ftd-fp2k.6.2.0.140-307i.SSA      6.2(0.140-307i)
cisco-ftd-fp2k.6.2.0.140-308i.SSA      6.2(0.140-308i)
cisco-ftd-fp2k.6.2.0.175-311i.SSA      6.2(0.175-311i)
cisco-ftd-fp2k.6.2.0.175-314i.SSA      6.2(0.175-314i)
cisco-ftd-fp2k.6.2.0.175-318i.SSA      6.2(0.175-318i)
cisco-ftd-fp2k.6.2.0.175-319i.SSA      6.2(0.175-319i)
```

show package package name expand

パッケージの詳細を表示します。

```
firepower /firmware # show package cisco-ftd-fp2k.6.2.0.131-303i.SSA expand
Package cisco-ftd-fp2k.6.2.0.131-303i.SSA:
Images:
  cisco-ftd.6.2.0.131.csp
  fxos-k8-fp2k-firmware.0.4.04.SPA
  fxos-k8-fp2k-lfbff.82.1.1.303i.SSA
  fxos-k8-fp2k-npu.82.1.1.303i.SSA
  fxos-k9-fp2k-manager.82.1.1.303i.SSA
```

scope auto-install

自動インストール モードを開始します。このモードでは、現在の FXOS のアップグレード状態を表示できます。

```
firepower /firmware/auto-install # show
Firmware Auto-Install:
Package-Vers Oper State Upgrade State
-----
6.2(0.175-319i) Scheduled Installing Application
```

scope firmware

ファームウェア モードを開始します。このモードでは、ダウンロード タスクに関する情報を表示できます。

次に例を示します。

```
FPR2100 /firmware # show download-task
Download task:
File Name                                     Protocol Server
Port      Userid      State
-----
cisco-ftd-fp2k.6.2.0.175-314i.SSA           Scp      172.29.191.78
0 danp      Downloaded
cisco-ftd-fp2k.6.2.0.175-318i.SSA           Scp      172.29.191.78
0 danp      Downloaded
cisco-ftd-fp2k.6.2.0.175-319i.SSA           Scp      172.29.191.78
0 danp      Downloaded
```

scope download-task

ダウンロード タスク モードを開始します。このモードでは、各ダウンロード タスクの詳細を表示してダウンロード タスクを再開できます。

次に例を示します。

```

Download task:
  File Name: test.SSA
  Protocol: Scp
  Server: 172.29.191.78
  Port: 0
  Userid: user
  Path: /tmp
  Downloaded Image Size (KB): 0
  Time stamp: 2016-11-15T19:42:29.854
  State: Failed
  Transfer Rate (KB/s): 0.000000
  Current Task: deleting downloadable test.SSA on
local(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:DeleteLocal)
firepower /firmware/download-task # show fsm status
File Name: test.SSA
FSM 1:
  Remote Result: End Point Failed
  Remote Error Code: ERR MO Illegal Iterator State
  Remote Error Description: End point timed out. Check for IP, port, password,
disk space or network access related issues.#
  Status: Download Fail
  Previous Status: Download Fail
  Timestamp: 2016-11-15T19:42:29.854
  Try: 2
  Progress (%): 0
  Current Task: deleting downloadable test.SSA on
local(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:DeleteLocal)

  firepower /firmware/download-task # restart
  Password:

```

scope psu

電源ユニットモードを開始します。このモードでは、電源ユニットに関する詳細情報を表示できます。

次に例を示します。

```

FPR2100 /chassis # show psu expand detail
PSU:
  PSU: 1
  Overall Status: Powered Off
  Operability: Unknown
  Power State: Off
  Presence: Equipped
  Voltage Status: Unknown
  Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
  PID: FPR2K-PWR-AC-400
  VID: V01
  Vendor: Cisco Systems, Inc
  Serial (SN): LIT2010CAFE
  Type: AC
  Fan Status: Ok
  PSU: 2
  Overall Status: Operable
  Operability: Operable
  Power State: On
  Presence: Equipped
  Voltage Status: Ok
  Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
  PID: FPR2K-PWR-AC-400
  VID: V01
  Vendor: Cisco Systems, Inc
  Serial (SN): LIT2010CAFE
  Type: AC
  Fan Status: Ok

```

Cisco Secure Firewall 3100 の connect local-mgmt トラブルシューティング コマンド

以下のこのセクションでは、既存のデバッグコマンドに加えて、Cisco Secure Firewall 3100 に固有の CLI について説明します。

Cisco Secure Firewall 3100 に関する問題をトラブルシューティングするには、以下の connect local-mgmt モード FXOS CLI コマンドを使用します。connect local-mgmt モードにアクセスするには、次のように入力します。

FPR3100# **connect local-mgmt**

show portmanager

スイッチ、パケット、SFP-FECカウンタ、デジタルオプティカルモニタリング (DOM)、QOS 機能、CPSS AP、およびサイクリックログダンプに関する詳細情報を表示します。

次に例を示します。

次の CLI は、vtcam-tti の FXOS ポートマネージャ スイッチ ハードウェア TCAM ルールダンプを表示します。

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware vtcam-tti
detail
VTCAM_RULE_ID  VLAN  SRC_PORT  PORTCHANNEL_ID  FLAGS  MODE  REF_COUNT
1              21      0          2              0      2      5          3
2             3078      0          0              0      0      0          1
3             3077      0          0              0      0      0          1
4             3076      0          0              0      0      0          1
5             3075      0          0              0      0      0          1
6             3074      0          0              0      0      0          1
7             3073      0          0              0      0      0          1
8              1      0          0              0      0      0          1
9             18     102          0              0     24      8          1
10             5     157          0              0     24      8          1
11             31      0          12              0      2      5          3
12             15     105          0              0     24      8          1
13              9     111          0              0     24      8          1
14             13     107          0              0     24      8          1
15             26      0          7              0      2      5          3
16             29      0          10             0      2      5          3
17             23      0          4              0      2      5          3
18             19     101          0              0     24      8          1
19             30      0          11             0      2      5          3
20             28      0          9              0      2      5          3
21              4     156          0              0     24      8          1
22             34      0          15             0      2      5          3
23              6     158          0              0     24      8          1
24              8     112          0              0     24      8          1
25             24      0          5              0      2      5          3
26             14     106          0              0     24      8          1
27             32      0          13             0      2      5          3
28             25      0          6              0      2      5          3
29             12      0          0              9      6      5          2
30             20      0          1              0      2      5          3
31             11     109          0              0     24      8          1
32             27      0          8              0      2      5          3
33             17     103          0              0     24      8          1
```

```

34          22      0      3          0      2      5      3
35          16     104     0          0     24      8      1
36           3       0     19          0     26      8      1
37          35       0     16          0      2      5      3
38          33       0     14          0      2      5      3
39           7     159      0          0     24      8      1
40           2       0     17          0     26      8      1
41          10     110      0          0     24      8      1

```

次の CLI は、FXOS ポート マネージャ スイッチの VLAN 出力を表示します。

```

firepower-3140(local-mgmt)# show portmanager switch vlans
VLAN                               Ports                               Tag           MAC-Learning
FDB-mode
-----
1                               0/17,19                           pop_outer_tag  Control
FID
2                               0/1-16,18                         outer_tag0_inner_tag1  Control
FID
                               0/20                               pop_outer_tag
3                               0/1-16,18                         outer_tag0_inner_tag1  Control
FID
4                               0/1-16,18                         outer_tag0_inner_tag1  Control
FID
5                               0/1-16,18                         outer_tag0_inner_tag1  Control
FID
6                               0/1-16,18                         outer_tag0_inner_tag1  Control
FID
7                               0/1-16,18                         outer_tag0_inner_tag1  Control
FID
8                               0/1-16,18                         outer_tag0_inner_tag1  Control
FID

```

次の CLI は、ポートチャネル インターフェイスのサマリーを確認するのに役立ちます。

```

firepower-3140(local-mgmt)# show por
portchannel portmanager

firepower-3140(local-mgmt)# show portchannel summary
Flags:  D - Down          P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met

-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
3    Po3 (U)      Eth       LACP      Eth1/3 (P)
2    Po2 (U)      Eth       LACP      Eth1/2 (P)

LACP KeepAlive Timer:
-----
Channel  PeerKeepAliveTimerFast
-----
3    Po3 (U)      False
2    Po2 (U)      False

Cluster LACP Status:

```



```

-----
Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID
-----
3      Po3 (U)      False      False      0
2      Po2 (U)      False      False      0
</pre>

```

次の CLI は、ポート チャネル ロードバランシング方式を表示します。

```

firepower-3140(local-mgmt)# show portchannel load-balance
PortChannel Load-Balancing Configuration:
  src-dst ip-l4port
PortChannel Load-Balancing Configuration Used Per-Protocol:
Non-IP: src-dst mac
  IP: src-dst ip-l4port
</pre>

```

次の CLI は、FXOS システムプロセスのステータスを表示します。

```

firepower-3140(local-mgmt)# show pmon state

```

SERVICE NAME	STATE	RETRY (MAX)	EXITCODE	SIGNAL	CORE
svc_sam_dme	running	0 (4)	0	0	no
svc_sam_dcosAG	running	0 (4)	0	0	no
svc_sam_portAG	running	0 (4)	0	0	no
svc_sam_statsAG	running	0 (4)	0	0	no
httpd.sh	running	0 (4)	0	0	no
svc_sam_sessionmgrAG	running	0 (4)	0	0	no
sam_core_mon	running	0 (4)	0	0	no
svc_sam_svcmonAG	running	0 (4)	0	0	no
svc_sam_serviceOrchAG	running	0 (4)	0	0	no
svc_sam_appAG	running	0 (4)	0	0	no
svc_sam_envAG	running	0 (4)	0	0	no
svc_sam_npuAG	running	0 (4)	0	0	no
svc_sam_eventAG	running	0 (4)	0	0	no

次の CLI は、イーサネット 1/1 ポートに一致する vtcam-tti ステージのスイッチハードウェア TCAM ルールダンプを表示します。

```

firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware vtcam-tti
ethernet 1 1

```

RULE_ID	VLAN	SRC_PORT	PC_ID	SRC_ID	MODE	PAK_CNT
1	20	0	1	0	101	0

次の CLI は、vlan 0 に一致する vtcam-tti ステージのスイッチハードウェア TCAM ルールダンプを表示します。

```

firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware vtcam-tti
vlan 0

```

RULE_ID	VLAN	SRC_PORT	PC_ID	SRC_ID	MODE	PAK_CNT
1	2	0	17	0	17	0
2	3	0	19	0	19	0
3	4	0	16	0	0	0
4	5	0	15	0	0	0
5	6	0	14	0	0	0
6	7	0	13	0	0	0
7	8	0	12	0	0	0
8	9	0	11	0	0	0
9	10	0	10	0	0	0
10	11	0	9	0	0	0
11	12	0	8	0	0	0
12	13	0	7	0	0	0

13	14	0	6	0	0	0	0
14	15	0	5	0	0	0	0
15	16	0	4	0	0	0	0
16	17	0	3	0	0	0	0
17	18	0	2	0	0	0	0
18	19	0	1	0	0	0	0
19	20	0	1	0	101	0	166
20	21	0	2	0	102	0	1597
21	22	0	3	0	103	0	0
22	23	0	4	0	104	0	0
23	24	0	5	0	105	0	0
24	25	0	6	0	106	0	0
25	26	0	7	0	107	0	0
26	27	0	8	0	108	0	0
27	28	0	9	0	109	0	0
28	29	0	10	0	110	0	0
29	30	0	11	0	111	0	0
30	31	0	12	0	112	0	0
31	32	0	13	0	159	0	0
32	33	0	14	0	158	0	0
33	34	0	15	0	157	0	0
34	35	0	16	0	156	0	0
35	1	0	17	0	0	0	0

次の CLI は、ハードウェア MAC フィルタ/EM ステージルールに関する詳細情報を表示します。

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter detail
```

```
EM Entry-No : 1
```

```
VLAN : 0
SRC_PORT : 17
PC_ID : 0
SRC_ID : 17
DST_PORT : 19
HW_ID : 3072
ACT_CMD : 0
PCL_ID : 1
REDIRECT_CMD : 1
BYPASS_BRG : 1
CND_INDEX : 3074
PACKET_COUNT : 1977
DMAC : 00:00:00:00:00:00
```

```
EM Entry-No : 2
```

```
VLAN : 0
SRC_PORT : 19
PC_ID : 0
SRC_ID : 19
DST_PORT : 17
HW_ID : 3074
ACT_CMD : 0
PCL_ID : 1
REDIRECT_CMD : 1
BYPASS_BRG : 1
CND_INDEX : 3075
PACKET_COUNT : 1858
DMAC : 00:00:00:00:00:00
```

次の CLI は、イーサネット 1/9 ポートに一致する MAC フィルタステージのスイッチハードウェア TCAM ルールダンプを表示します。

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
ethernet 1 9
VLAN    SRC_PORT    PC_ID    SRC_ID    DST_PORT    PKT_CNT    DMAC
1        0           9        0         109        1536       0 1:80:c2:0:0:2
```

次の CLI は、ソフトウェア MAC フィルタに関する詳細情報を表示します。

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules software mac-filter
detail
VLAN    SRC_PORT    PORTCHANNEL_ID    DST_PORT    FLAGS    MODE    DMAC
1        0           17                0           19       26      8 0:0:0:0:0:0
2        0           9                 0           1536     2       5 1:80:c2:0:0:2
3        104         0                 0           4        24      8 0:0:0:0:0:0
4        0           7                 0           1536     2       5 1:80:c2:0:0:2
5        101         0                 0           1        24      8 0:0:0:0:0:0
6        0           1                 0           1536     2       5 1:80:c2:0:0:2
7        0           3                 0           1536     2       5 1:80:c2:0:0:2
8        106         0                 0           6        24      8 0:0:0:0:0:0
9        158         0                 0           14       24      8 0:0:0:0:0:0
10       0           13                0           1536     2       5 1:80:c2:0:0:2
11       0           14                0           1536     2       5 1:80:c2:0:0:2
12       0           6                 0           1536     2       5 1:80:c2:0:0:2
13       0           8                 0           1536     2       5 1:80:c2:0:0:2
14       112         0                 0           12       24      8 0:0:0:0:0:0
15       107         0                 0           7        24      8 0:0:0:0:0:0
16       0           19                0           17       26      8 0:0:0:0:0:0
17       0           12                0           1536     2       5 1:80:c2:0:0:2
18       0           5                 0           1536     2       5 1:80:c2:0:0:2
19       102         0                 0           2        24      8 0:0:0:0:0:0
20       156         0                 0           16       24      8 0:0:0:0:0:0
21       103         0                 0           3        24      8 0:0:0:0:0:0
22       0           11                0           1536     2       5 1:80:c2:0:0:2
23       157         0                 0           15       24      8 0:0:0:0:0:0
24       111         0                 0           11       24      8 0:0:0:0:0:0
25       0           10                0           1536     2       5 1:80:c2:0:0:2
26       108         0                 0           8        24      8 0:0:0:0:0:0
27       159         0                 0           13       24      8 0:0:0:0:0:0
28       110         0                 0           10       24      8 0:0:0:0:0:0
29       105         0                 0           5        24      8 0:0:0:0:0:0
30       0           2                 0           1536     2       5 1:80:c2:0:0:2
31       0           4                 0           1536     2       5 1:80:c2:0:0:2
32       0           16                0           1536     2       5 1:80:c2:0:0:2
33       109         0                 0           9        24      8 0:0:0:0:0:0
34       0           15                0           1536     2       5 1:80:c2:0:0:2
```

次の CLI は、イーサネット 1/9 ポートに一致する MAC フィルタステージのスイッチソフトウェア DB ルールを表示します。

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules software mac-filter
ethernet 1 9
VLAN    SRC_PORT    PORTCHANNEL_ID    DST_PORT    FLAGS    MODE    DMAC
1        0           9                 0           1536     2       5 1:80:c2:0:0:2
```

次の CLI は、スイッチブリッジエンジンのパケットドロップに関する詳細情報を表示します。

```
firepower-3140(local-mgmt)# show portmanager switch counters bridge
```

```
Bridge Ingress Drop Counter: 2148
No Bridge Ingress Drop
```

次の CLI は、ハードウェアスイッチのパケットカウンタの詳細を表示します。

```
firepower-3140(local-mgmt)# show portmanager switch counters packet-trace
```

Counter	Description	
goodOctetsRcv	Number of ethernet frames received that are not bad ethernet frames or MAC Control pkts	
badOctetsRcv	Sum of lengths of all bad ethernet frames received	
gtBrgInFrames	Number of packets received	
gtBrgVlanIngFilterDisc	Number of packets discarded due to VLAN Ingress Filtering	
gtBrgSecFilterDisc	Number of packets discarded due to Security Filtering measures	
gtBrgLocalPropDisc	Number of packets discarded due to reasons other than VLAN ingress and Security filtering	
dropCounter	Ingress Drop Counter	
outUcFrames	Number of unicast packets transmitted	
outMcFrames	Number of multicast packets transmitted. This includes registered multicasts, unregistered multicasts and unknown unicast packets	
outBcFrames	Number of broadcast packets transmitted	
brgEgrFilterDisc	Number of IN packets that were Bridge Egress filtered	
txqFilterDisc	Number of IN packets that were filtered due to TxQ congestion	
outCtrlFrames	Number of out control packets (to cpu, from cpu and to analyzer)	
egrFrwDropFrames	Number of packets dropped due to egress forwarding restrictions	
goodOctetsSent	Sum of lengths of all good ethernet frames sent from this MAC	
Counter	Source port- 0/0	Destination port- 0/0
goodOctetsRcv	---	---
badOctetsRcv	---	---
Ingress counters		
gtBrgInFrames	6650	6650
gtBrgVlanIngFilterDisc	0	0
gtBrgSecFilterDisc	0	0
gtBrgLocalPropDisc	0	0
dropCounter	2163	Only for source-port
Egress counters		
outUcFrames	0	0
outMcFrames	2524	2524
outBcFrames	1949	1949
brgEgrFilterDisc	14	14
txqFilterDisc	0	0
outCtrlFrames	0	0
egrFrwDropFrames	0	0
goodOctetsSent	---	---

次の CLI は、CPU のスイッチトラフィックに関する詳細情報を表示します。

```
firepower-3140(local-mgmt)# show portmanager switch traffic cpu
```

Dev/RX queue	packets	bytes
0/0	0	0
0/1	0	0
0/2	0	0

```

0/3          0          0
0/4          0          0
0/5          0          0
0/6          0          0
0/7          0          0          #

```

次の CLI は、ハードウェア スイッチ ポート トラフィックの詳細を表示します。

```
firepower-3140(local-mgmt)# show portmanager switch traffic port
```

```

max-rate - pps that the port allow with packet size=64
actual-tx-rate - pps that egress the port (+ % from 'max')
actual-rx-rate - pps that ingress the port(+ % from 'max')

```

Dev/Port	max-rate	actual-tx-rate	actual-rx-rate
0/1	1488095	(0%)---	(0%)---
0/2	1488095	(0%)---	(0%)---
0/3	14880	(0%)---	(0%)---
0/4	14880	(0%)---	(0%)---
0/5	14880	(0%)---	(0%)---
0/6	14880	(0%)---	(0%)---
0/7	14880	(0%)---	(0%)---
0/8	14880	(0%)---	(0%)---
0/9	14880952	(0%)---	(0%)---
0/10	14880952	(0%)---	(0%)---
0/11	14880952	(0%)---	(0%)---
0/12	14880952	(0%)---	(0%)---
0/13	14880952	(0%)---	(0%)---
0/14	14880952	(0%)---	(0%)---
0/15	1488095	(0%)---	(0%)---
0/16	1488095	(0%)---	(0%)---
0/17	14880952	(0%)---	(0%)---
0/18	74404761	(0%)---	(0%)---
0/19	37202380	(0%)---	(0%)---
0/20	37202380	(0%)---	(0%)---

次の CLI は、イーサネット 1/13 ポートに一致する SFP-FEC カウンタに関する詳細情報を表示します。

```

firepower-3140(local-mgmt)# show portmanager counters ethernet 1 13
  Good Octets Received          : 2153
  Bad Octets Received           : 0
  MAC Transmit Error           : 0
  Good Packets Received         : 13
  Bad packets Received          : 0
  BRDC Packets Received         : 0
  MC Packets Received           : 13
  .....
  .....
  txqFilterDisc                 : 0
  linkchange                     : 1
  FcFecRxBlocks                 : 217038081
  FcFecRxBlocksNoError          : 217038114
  FcFecRxBlocksCorrectedError   : 0
  FcFecRxBlocksUnCorrectedError : 0
  FcFecRxBlocksCorrectedErrorBits : 0
  FcFecRxBlocksCorrectedError0   : 0
  FcFecRxBlocksCorrectedError1   : 0
  FcFecRxBlocksCorrectedError2   : 0
  FcFecRxBlocksCorrectedError3   : 0

```

```

FcFecRxBlocksUncorrectedError0      : 0
FcFecRxBlocksUncorrectedError1      : 0
FcFecRxBlocksUncorrectedError2      : 0
FcFecRxBlocksUncorrectedError3      : 0

```

次の CLI は、イーサネット 1/14 ポートに一致する SFP-FEC カウンタに関する詳細情報を表示します。

```

firepower-3140(local-mgmt)# show portmanager counters ethernet 1 14
Good Octets Received                  : 2153
Bad Octets Received                   : 0
MAC Transmit Error                   : 0
Good Packets Received                 : 13
Bad packets Received                  : 0
BRDC Packets Received                 : 0
MC Packets Received                   : 13
.....
.....
txqFilterDisc                         : 0
linkchange                           : 1
RsFeccorrectedFecCodeword             : 0
RsFecuncorrectedFecCodeword           : 10
RsFecsymbolError0                     : 5
RsFecsymbolError1                     : 0
RsFecsymbolError2                     : 0
RsFecsymbolError3                     : 0

```

次の CLI は、イーサネット 1/5 ポートに一致するデジタル オプティカル モニタリング (DOM) 情報に関する詳細情報を表示します。

```

firepower-4245(local-mgmt)# show portmanager port-info ethernet 1 5
....
....
DOM info:
=====:

Status/Control Register: 0800
    RX_LOS State: 0
    TX_FAULT State: 0
Alarm Status: 0000
No active alarms
Warning Status: 0000
No active warnings

THRESHOLDS
alarm
high alarm    high warning    low warning    low
-05.000      Temperature    C    +075.000      +070.000      +000.000
002.9700     Voltage        V    003.6300      003.4650      003.1350
001.0000     Bias Current   mA    012.0000      011.5000      002.0000
001.0000     Transmit power mW    034.6740      017.3780      002.5120
000.5370     Receive power  mW    034.6740      017.3780      001.3490

Environmental Information - raw values
Temperature: 38.84 C

```

```

Supply voltage: 33703 in units of 100uVolt
Tx bias: 3499 in units of 2uAmp
Tx power: 0.1 dBm (10251 in units of 0.1 uW)
Rx power: -0.9 dBm (8153 in units of 0.1 uW)
DOM (256 bytes of raw data in hex)
=====
0x0000 : 4b 00 fb 00 46 00 00 00 8d cc 74 04 87 5a 7a 76
0x0010 : 17 70 01 f4 16 76 03 e8 87 72 03 e8 43 e2 09 d0
0x0020 : 87 72 02 19 43 e2 05 45 00 00 00 00 00 00 00 00
0x0030 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0040 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0050 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 86
0x0060 : 26 54 83 a7 0d ab 28 0b 1f d9 00 00 00 00 00 00
0x0070 : 00 00 03 00 00 00 00 00 00 08 f3 00 00 00 00 01
0x0080 : 49 4e 55 49 41 43 53 45 41 41 31 30 2d 33 33 38
0x0090 : 38 2d 30 31 56 30 31 20 01 00 46 00 00 00 00 e3
0x00a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00c0 : 53 46 50 2d 31 30 2f 32 35 47 2d 43 53 52 2d 53
0x00d0 : 20 20 20 20 30 38 00 00 00 00 00 00 00 00 00 d1
0x00e0 : 1e 20 2a 2a 31 34 29 36 00 00 00 00 00 00 00 00
0x00f0 : 00 00 00 00 00 56 00 00 ff ff ff ff 00 00 00 cf
=====
PHY Data:
PAGE IFC OFFSET VALUE | PAGE IFC OFFSET VALUE
-----

```

次の CLI は、パケットキャプチャのパラメータ設定に関する詳細情報を表示します。

```

firepower-3140(local-mgmt)# show portmanager switch pktpcap-rules software
Software DB rule:1
Slot= 1
Interface= 12
Breakout-port= 0
Protocol= 6
Ethertype= 0x0000
Filter_key= 0x00000040
Session= 1
Vlan= 0
SrcPort= 0
DstPort= 0
SrcIp= 0.0.0.0
DstIp= 0.0.0.0
SrcIpv6= ::
DestIpv6= ::
SrcMacAddr= 00:00:00:00:00:00
DestMacAddr= 00:00:00:00:00:00

```

次の CLI は、FXOS ポートマネージャスイッチのハードウェア TCAM ルールに関する詳細情報を表示します。

```

firepower-3140(local-mgmt)# show portmanager switch pktpcap-rules hardware
Hardware DB rule:1
Hw_index= 15372
Rule_id= 10241
Cnc_index= 1
Packet_count= 0
Slot= 1
Interface= 12
Protocol= 6
Ethertype= 0x0000
Vlan= 0
SrcPort= 0

```

```

DstPort= 0
SrcIp= 0.0.0.0
DstIp= 0.0.0.0
SrcIpv6= ::
DestIpv6= ::
SrcMacAddr= 00:00:00:00:00:00
DestMacAddr= 00:00:00:00:00:00

```

以下は、QOS 機能に関する詳細情報を表示します。

```

firepower(local-mgmt)# show portmanager switch qos-rule policer counters
Policer_type    green(pass_count)    yellow(pass_count)    red(drop_count)
-----
OSPF              102025351              17832                  590
780
Policer_type    green(pass_count)    yellow(pass_count)    red(drop_count)
-----
CCL_CLU           0                      0                      0
Policer_type    green(pass_count)    yellow(pass_count)    red(drop_count)
-----
BFD              61343307              0                      0
Policer_type    green(pass_count)    yellow(pass_count)    red(drop_count)
-----
HA                0                      0                      0
Policer_type    green(pass_count)    yellow(pass_count)    red(drop_count)
-----
CCL_CONTROL       0                      0                      0

```

次の CLI は、優先順位の高いトラフィックが TCAM に到達しているかどうかを確認します。

```

firepower(local-mgmt)# show portmanager switch qos-rule counters
Rule_no  Rule_id  Rule_type  pass_count
-----
1         9218     SW_QOS_BFD      0
Rule_no  Rule_id  Rule_type  pass_count
-----
2         9216     SW_QOS_OSPF    102633941
Rule_no  Rule_id  Rule_type  pass_count
-----
3         9217     SW_QOS_BFD    61343307

```

次の CLI は、イーサネット 1/10 ポートに一致するデバイスのキューごとの CPU 統計を表示します。

```

firepower(local-mgmt)# show queuing interface ethernet 1 10
Queue    Traffic-type    Scheduler-type    oper-bandwidth    Destination
-----
3         Data            WRR              100              Application
4         CCL-CLU         SP              0              Application
5         BFD            SP              0              Application
6         OSPF           SP              0              Application
7  CCL-CONTROL/HA/LACP_Tx  SP              0              Application
0  packet-capture    N/A             0              CPU
7         LACP_Rx        N/A             0              CPU
Port 1/10 Queue Statistics:
Queue 0:
  Number of packets passed : 0
  Number of packets dropped: 0

```



```

Queue 1:
  Number of packets passed :          0
  Number of packets dropped:          0
Queue 2:
  Number of packets passed :          0
  Number of packets dropped:          0
Queue 3:
  Number of packets passed :      466420167
  Number of packets dropped:          0
Queue 4:
  Number of packets passed :          0
  Number of packets dropped:          0
Queue 5:
  Number of packets passed :          0
  Number of packets dropped:          0
Queue 6:
  Number of packets passed :      41536261
  Number of packets dropped:          0
Queue 7:
  Number of packets passed :         912
  Number of packets dropped:          0
CPU Statistics:
Queue 2:
  Number of packets passed :      180223
  Number of packets dropped:          0
Queue 7:
  Number of packets passed :         1572
  Number of packets dropped:          0

```

次の CLI は、内部 1/1 ポートに一致するデバイスのキューごとの CPU 統計を表示します。

```

firepower(local-mgmt)# show queuing interface internal 1 1
Queue      Traffic-type      Scheduler-type  oper-bandwidth  Destination
-----
3          Data              WRR              100             Application
4          CCL-CLU                SP                0             Application
5          BFD                    SP                0             Application
6          OSPF                  SP                0             Application
7  CCL-CONTROL/HA/LACP_Tx    SP                0             Application
0  packet-capture            N/A              0             CPU
7          LACP_Rx            N/A              0             CPU
Port 1/18 Queue Statistics:
Queue 0:
  Number of packets passed :          0
  Number of packets dropped:          0
Queue 1:
  Number of packets passed :          0
  Number of packets dropped:          0
Queue 2:
  Number of packets passed :          0
  Number of packets dropped:          0
Queue 3:
  Number of packets passed :          17
  Number of packets dropped:          0
Queue 4:
  Number of packets passed :          0
  Number of packets dropped:          0
Queue 5:
  Number of packets passed :          0
  Number of packets dropped:          0
Queue 6:
  Number of packets passed :         5151

```

```

      Number of packets dropped:          0
Queue 7:
      Number of packets passed :          17345
      Number of packets dropped:          0
CPU Statistics:
Queue 2:
      Number of packets passed :          180223
      Number of packets dropped:          0
Queue 7:
      Number of packets passed :          1572
      Number of packets dropped:          0
Note:The CPU statistics are per Queue per Device

```

次の CLI は、ダンプ AP ログオプションに関する詳細情報を表示します。

```

firepower-3110(local-mgmt)# dump portmanager switch ap-log
requested log has been dumped to /opt/cisco/platform/logs/portmgr.out*

firepower-3110(local-mgmt)# dump portmanager switch cyclic-log
requested log has been dumped to /opt/cisco/platform/logs/portmgr.out*

```

次の CLI は、ポートマネージャの詳細ログの有効化または無効化に関する詳細情報を表示します。

```

firepower-3110(local-mgmt)# debug portmanager switch
all Enable or Disable verbose logging for switch

firepower-3110(local-mgmt)# debug portmanager switch all
firepower-3110(local-mgmt)#

firepower-3110(local-mgmt)# no debug portmanager switch all
firepower-3110(local-mgmt)#

```

次の CLI は、8つのトラフィッククラス/キューのポートベースのパケットドロップに関する詳細情報を表示します。

```

firepower-3110(local-mgmt)# show portmanager switch tail-drop-allocated buffers all
-----

```

Per Port and Traffic Class								
Port	Per port	TC0	TC1	TC2	TC3	TC4	TC5	TC6
0/1	10	10	10	10	10	10	10	10
0/2	15	15	15	15	10	10	10	10
0/3	10	10	10	10	10	10	10	10
0/4	80	10	10	10	10	10	10	10
0/5	10	10	10	10	10	10	10	10
0/6	10	10	10	10	10	10	10	10
0/7	200	25	25	150	10	10	25	150

```

      |25      |
0/8  |0      |0      |0      |0      |0      |0      |0
      |0      |
-----

```

次の CLI は、tti-lookup0 が原因でドロップされたパケット数を表示します。

```

firepower-3110(local-mgmt)# show portmanager switch default-rule-drop-counter
tti-lookup0

```

Rule_id	cnc_index	packet_count
1	1	4

次の CLI は、ipcl-lookup0 が原因でドロップされたパケット数を表示します。

```

firepower-3110(local-mgmt)# show portmanager switch default-rule-drop-counter
ipcl-lookup0

```

Rule_id	cnc_index	packet_count
4096	0	114

アプライアンスモードでの Cisco Secure Firepower 4200 の connect local-mgmt トラブルシューティング コマンド

以下のこのセクションでは、既存のデバッグコマンドに加えて、Cisco Secure Firewall 3100 に固有の CLI について説明します。

アプライアンスモードで Cisco Secure Firewall 3100 に関する問題をトラブルシューティングするには、以下の connect local-mgmt モード FXOS CLI コマンドを使用します。connect local-mgmt モードにアクセスするには、次のように入力します。

FPR 4200# **connect local-mgmt**

show portmanager

スイッチ、パケット、SFP-FECカウンタ、デジタルオプティカルモニタリング (DOM)、QOS 機能、CPSS AP、およびサイクリックログダンプに関する詳細情報を表示します。次に例を示します。

次の CLI は、vtcam-tti の FXOS ポートマネージャ スイッチ ハードウェア TCAM ルールダンプを表示します。

```

firepower(local-mgmt)# show portmanager switch forward-rules hardware vtcam-tti

```

	RULE_ID	VLAN	NUM_MPLS_LABELS	SRC_PORT	PC_ID	SRC_ID	MODE	PAK_CNT
1	2	0	0	10	0	10	0	1951
2	3	0	0	14	0	14	0	19
3	4	0	0	9	0	9	0	227505
4	5	0	0	13	0	13	0	103587
5	6	0	0	8	0	0	0	0
6	7	0	0	7	0	0	0	0
7	8	0	0	6	0	0	0	0
8	9	0	0	5	0	0	0	0
9	10	0	0	4	0	0	0	0

アプライアンスモードでの Cisco Secure Firepower 4200 の connect local-mgmt トラブルシューティングコマンド

10	11	0	0	3	0	0	0	0
11	12	0	0	2	0	0	0	0
12	13	0	0	1	0	0	0	607
13	14	0	0	44	0	0	0	0
14	15	0	0	40	0	0	0	0
15	16	0	0	36	0	0	0	0
16	17	0	0	32	0	0	0	0
17	30	0	0	1	0	101	1	2120
18	18	0	0	1	0	101	0	306
19	19	0	0	2	0	102	0	2429
20	20	0	0	3	0	103	0	0
21	21	0	0	4	0	104	0	0
22	22	0	0	5	0	105	0	0
23	23	0	0	6	0	106	0	0
24	24	0	0	7	0	107	0	0
25	25	0	0	8	0	108	0	0
26	26	0	0	32	0	117	0	0
27	27	0	0	36	0	121	0	0
28	28	0	0	40	0	125	0	0
29	29	0	0	44	0	129	0	0
30	1	0	0	9	0	0	0	1875
31	8193	0	1	0	0	0	0	0
32	8194	0	2	0	0	0	0	0
33	8195	0	3	0	0	0	0	0
34	8196	0	4	0	0	0	0	0
35	8197	0	5	0	0	0	0	0
36	8198	0	6	0	0	0	0	0

次の CLI は、vlan 0 に一致する vtcam-tti ステージのスイッチハードウェア TCAM ルール ダンプを表示します。

```
firepower(local-mgmt)# show portmanager switch forward-rules hardware vtcam-tti
```

	RULE_ID	VLAN	NUM_MPLS_LABELS	SRC_PORT	PC_ID	SRC_ID	MODE	PAK_CNT
1	2	0	0	10	0	10	0	1961
2	3	0	0	14	0	14	0	19
3	4	0	0	9	0	9	0	227517
4	5	0	0	13	0	13	0	103683
5	6	0	0	8	0	0	0	0
6	7	0	0	7	0	0	0	0
7	8	0	0	6	0	0	0	0
8	9	0	0	5	0	0	0	0
9	10	0	0	4	0	0	0	0
10	11	0	0	3	0	0	0	0
11	12	0	0	2	0	0	0	0
12	13	0	0	1	0	0	0	617
13	14	0	0	44	0	0	0	0
14	15	0	0	40	0	0	0	0
15	16	0	0	36	0	0	0	0
16	17	0	0	32	0	0	0	0
17	30	0	0	1	0	101	1	2156
18	18	0	0	1	0	101	0	306
19	19	0	0	2	0	102	0	2466
20	20	0	0	3	0	103	0	0
21	21	0	0	4	0	104	0	0
22	22	0	0	5	0	105	0	0
23	23	0	0	6	0	106	0	0
24	24	0	0	7	0	107	0	0
25	25	0	0	8	0	108	0	0
26	26	0	0	32	0	117	0	0
27	27	0	0	36	0	121	0	0
28	28	0	0	40	0	125	0	0
29	29	0	0	44	0	129	0	0

```

30          1      0      0          9      0      0      0      1875
31      8193      0      1          0      0      0      0          0
32      8194      0      2          0      0      0      0          0
33      8195      0      3          0      0      0      0          0
34      8196      0      4          0      0      0      0          0
35      8197      0      5          0      0      0      0          0
36      8198      0      6          0      0      0      0          0

```

次の CLI は、イーサネット 1/9 ポートに一致する MAC フィルタステージのスイッチハードウェア TCAM ルールダンプを表示します。

```

firepower(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN  SRC_PORT  PC_ID  SRC_ID  DST_PORT  PKT_CNT  DMAC
1         0         44      0      129      1536        0  1:80:c2:0:0:2
2         0         44      0      129      1536        0  ff:ff:ff:ff:ff:ff
3         0          2      0      102      1536        0  ba:db:ad:f0:2:8f
4         0          4      0      104      1536        0  ff:ff:ff:ff:ff:ff
5         0          4      0      104      1536        0  1:80:c2:0:0:2
6         0          5      0      105      1536        0  1:80:c2:0:0:2
7         0          5      0      105      1536        0  ff:ff:ff:ff:ff:ff
8         0         13      0       13          9      103735  0:0:0:0:0:0
9         0         32      0      117      1536        0  ba:db:ad:f0:2:9e
10        0          7      0      107      1536        0  ff:ff:ff:ff:ff:ff
11        0          7      0      107      1536        0  1:80:c2:0:0:2
12        0          6      0      106      1536        0  1:80:c2:0:0:2
13        0          6      0      106      1536        0  ff:ff:ff:ff:ff:ff
14        0         14      0       14         10         19  0:0:0:0:0:0
15        0         10      0       10         14      1979  0:0:0:0:0:0
16        0         44      0      129      1536        0  ba:db:ad:f0:2:a1
17        0          9      0       9         13      1227537  0:0:0:0:0:0
18        0          8      0      108      1536        0  1:80:c2:0:0:2
19        0          8      0      108      1536        0  ff:ff:ff:ff:ff:ff
20        0          1      0      101      1536        0  ff:ff:ff:ff:ff:ff
21        0          1      0      101      1536        0  1:80:c2:0:0:2
22        0          3      0      103      1536        0  1:80:c2:0:0:2
23        0          1      0      101      1536      2183  1:0:0:0:0:0
24        0          3      0      103      1536        0  ff:ff:ff:ff:ff:ff
25        0          2      0      102      1536        23  ff:ff:ff:ff:ff:ff
26        0          2      0      102      1536        0  1:80:c2:0:0:2
27        0         32      0      117      1536        0  ff:ff:ff:ff:ff:ff
28        0         32      0      117      1536        0  1:80:c2:0:0:2
29        0         40      0      125      1536        0  ff:ff:ff:ff:ff:ff
30        0         40      0      125      1536        0  1:80:c2:0:0:2
31        0          7      0      107      1536        0  ba:db:ad:f0:2:94
32        0          5      0      105      1536        0  ba:db:ad:f0:2:92
33        0         36      0      121      1536        0  1:80:c2:0:0:2
34        0          4      0      104      1536        0  ba:db:ad:f0:2:91
35        0         36      0      121      1536        0  ff:ff:ff:ff:ff:ff
36        0          8      0      108      1536        0  ba:db:ad:f0:2:95
37        0          6      0      106      1536        0  ba:db:ad:f0:2:93
38        0          3      0      103      1536        0  ba:db:ad:f0:2:90
39        0         36      0      121      1536        0  ba:db:ad:f0:2:9f
40        0          1      0      101      1536       32  ba:db:ad:f0:2:8e
41        0         40      0      125      1536        0  ba:db:ad:f0:2:a0

```

次の CLI は、ソフトウェア MAC フィルタに関する詳細情報を表示します。

```

firepower-4225(local-mgmt)# show portmanager switch forward-rules software mac-filter
      NATIVE_VLAN  VLAN  SRC_PORT  PORTCHANNEL_ID  DST_PORT  FLAGS  MODE  DMAC
1              0    106          6              0    1536    2      5
1:80:c2:0:0:2

```

アプライアンスモードでの Cisco Secure Firepower 4200 の connect local-mgmt トラブルシューティングコマンド

2	0	105	5	0	1536	2	5
ff:ff:ff:ff:ff:ff							
3	0	105	5	0	1536	2	5
1:80:c2:0:0:2							
4	0	121	0	0	36	24	8
0:0:0:0:0:0							
5	0	106	6	0	1536	2	5
ff:ff:ff:ff:ff:ff							
6	0	121	36	0	1536	2	5
1:80:c2:0:0:2							
7	0	117	32	0	1536	2	5
1:80:c2:0:0:2							
8	0	125	40	0	1536	2	5
ff:ff:ff:ff:ff:ff							
9	0	129	0	0	44	24	8
0:0:0:0:0:0							
10	0	117	32	0	1536	2	5
ff:ff:ff:ff:ff:ff							
11	0	103	3	0	1536	2	5
1:80:c2:0:0:2							
12	0	102	2	0	1536	2	5
ff:ff:ff:ff:ff:ff							
13	0	117	0	0	32	24	8
0:0:0:0:0:0							
14	0	107	0	0	7	24	8
0:0:0:0:0:0							
15	0	101	1	0	1536	2	5
ba:db:ad:f0:2:8e							
16	0	107	7	0	1536	2	5
ff:ff:ff:ff:ff:ff							
17	0	106	6	0	1536	2	5
ba:db:ad:f0:2:93							
18	0	105	0	0	5	24	8
0:0:0:0:0:0							
19	0	102	0	0	2	24	8
0:0:0:0:0:0							
20	0	104	4	0	1536	2	5
ba:db:ad:f0:2:91							
21	0	107	7	0	1536	2	5
ba:db:ad:f0:2:94							
22	0	129	44	0	1536	2	5
1:80:c2:0:0:2							
23	0	102	2	0	1536	2	5
1:80:c2:0:0:2							
24	0	121	36	0	1536	2	5
ff:ff:ff:ff:ff:ff							
25	0	1	13	0	9	26	8
0:0:0:0:0:0							
26	0	108	8	0	1536	2	5
1:80:c2:0:0:2							
27	0	101	1	0	1536	2	5
ff:ff:ff:ff:ff:ff							
28	0	2	10	0	14	26	8
0:0:0:0:0:0							
29	0	101	1	0	1536	2	5
1:80:c2:0:0:2							
30	0	1	9	0	13	26	8
0:0:0:0:0:0							
31	0	129	44	0	1536	2	5
ff:ff:ff:ff:ff:ff							
32	0	125	0	0	40	24	8
0:0:0:0:0:0							
33	0	108	8	0	1536	2	5
ba:db:ad:f0:2:95							

```

34          0          2          14          0          10          26          8
0:0:0:0:0:0
35          0          129         44          0          1536          2          5
ba:db:ad:f0:2:a1
36          0          103          0          0          3          24          8
0:0:0:0:0:0
37          0          104          0          0          4          24          8
0:0:0:0:0:0
38          0          104          4          0          1536          2          5
ff:ff:ff:ff:ff:ff
39          0          107          7          0          1536          2          5
1:80:c2:0:0:2
40          0          104          4          0          1536          2          5
1:80:c2:0:0:2
41          0          101          1          0          1536          18          8
0:0:0:0:0:0
42          0          101          0          0          1          24          8
0:0:0:0:0:0
43          0          108          8          0          1536          2          5
ff:ff:ff:ff:ff:ff
44          0          121          36          0          1536          2          5
ba:db:ad:f0:2:9f
45          0          117          32          0          1536          2          5
ba:db:ad:f0:2:9e
46          0          105          5          0          1536          2          5
ba:db:ad:f0:2:92
47          0          125          40          0          1536          2          5
ba:db:ad:f0:2:a0
48          0          125          40          0          1536          2          5
1:80:c2:0:0:2
49          0          108          0          0          8          24          8
0:0:0:0:0:0
50          0          106          0          0          6          24          8
0:0:0:0:0:0
51          0          103          3          0          1536          2          5
ba:db:ad:f0:2:90
52          0          102          2          0          1536          2          5
ba:db:ad:f0:2:8f
53          0          103          3          0          1536          2          5
ff:ff:ff:ff:ff:ff

```

次の CLI は、スイッチブリッジエンジンのパケットドロップに関する詳細情報を表示します。

```

firepower-4225(local-mgmt)# show portmanager switch counters bridge
Bridge Ingress Drop Counter: 4688
No Bridge Ingress Drop

```

次の CLI は、ハードウェアスイッチのパケットカウンタの詳細を表示します。

```

how portmanager switch counters packet-trace

```

```

firepower-4225(local-mgmt)# show portmanager switch counters packet-trace

```

Counter	Description
goodOctetsRcv	Number of ethernet frames received that are not bad ethernet frames or MAC Control pkts
badOctetsRcv	Sum of lengths of all bad ethernet frames received
gtBrgInFrames	Number of packets received
gtBrgVlanIngFilterDisc	Number of packets discarded due to VLAN Ingress Filtering
gtBrgSecFilterDisc	Number of packets discarded due to Security Filtering measures

```

gtBrgLocalPropDisc    Number of packets discarded due to reasons other than
                      VLAN ingress and Security filtering
dropCounter           Ingress Drop Counter
outUcFrames            Number of unicast packets transmitted
outMcFrames            Number of multicast packets transmitted. This includes
                      registered multicasts, unregistered multicasts
                      and unknown unicast packets
outBcFrames            Number of broadcast packets transmitted
brgEgrFilterDisc       Number of IN packets that were Bridge Egress filtered
txqFilterDisc          Number of IN packets that were filtered
                      due to TxQ congestion
outCtrlFrames          Number of out control packets
                      (to cpu, from cpu and to analyzer)
egrFrwDropFrames       Number of packets dropped due to egress
                      forwarding restrictions
goodOctetsSent         Sum of lengths of all good ethernet
                      frames sent from this MAC

```

Counter	Source port- 0/0	Destination port- 0/0
goodOctetsRcv	---	---
badOctetsRcv	---	---
Ingress counters		
gtBrgInFrames	1341132	1341132
gtBrgVlanIngFilterDisc	0	0
gtBrgSecFilterDisc	0	0
gtBrgLocalPropDisc	0	0
dropCounter	4699	Only for source-port
Egress counters		
outUcFrames	1329593	1329593
outMcFrames	4594	4594
outBcFrames	2237	2237
brgEgrFilterDisc	9	9
txqFilterDisc	0	0
outCtrlFrames	0	0
egrFrwDropFrames	0	0
mcFifoDropPkts	0	0
mcFilterDropPkts	0	0
goodOctetsSent	---	---

次の CLI は、CPU のスイッチトラフィックに関する詳細情報を表示します。

```
firepower-4225(local-mgmt)# show portmanager switch traffic cpu
```

Dev/RX queue	packets	bytes
0/0	0	0
0/1	0	0
0/2	0	0
0/3	0	0
0/4	0	0
0/5	0	0
0/6	0	0
0/7	0	0

次の CLI は、ハードウェア スイッチ ポート トラフィックの詳細を表示します。


```
firepower-4225(local-mgmt)# show portmanager switch traffic port
```

```
max-rate - pps that the port allow with packet size=64
actual-tx-rate - pps that egress the port (+ % from 'max')
actual-rx-rate - pps that ingress the port(+ % from 'max')
```

Dev/Port	max-rate	actual-tx-rate	actual-rx-rate
0/1	1488095	(0%)---	(0%)---
0/2	1488095	(0%)---	(0%)---
0/3	14880	(0%)---	(0%)---
0/4	14880	(0%)---	(0%)---
0/5	14880	(0%)---	(0%)---
0/6	14880	(0%)---	(0%)---
0/7	14880	(0%)---	(0%)---
0/8	14880	(0%)---	(0%)---
0/9	14880952	(0%)---	(0%)---
0/10	14880952	(0%)---	(0%)---
0/11	14880952	(0%)---	(0%)---
0/12	14880952	(0%)---	(0%)---
0/13	14880952	(0%)---	(0%)---
0/14	14880952	(0%)---	(0%)---
0/15	1488095	(0%)---	(0%)---
0/16	1488095	(0%)---	(0%)---
0/17	14880952	(0%)---	(0%)---
0/18	74404761	(0%)---	(0%)---
0/19	37202380	(0%)---	(0%)---
0/20	37202380	(0%)---	(0%)---

次の CLI は、イーサネット 1/13 ポートに一致する SFP-FEC カウンタに関する詳細情報を表示します。

```
firepower-4225(local-mgmt)# show portmanager counters ethernet 1 13
Good Octets Received          : 2153
Bad Octets Received           : 0
MAC Transmit Error            : 0
Good Packets Received         : 13
Bad packets Received          : 0
BRDC Packets Received         : 0
MC Packets Received           : 13
.....
.....
txqFilterDisc                  : 0
linkchange                     : 1
FcFecRxBlocks                  : 217038081
FcFecRxBlocksNoError           : 217038114
FcFecRxBlocksCorrectedError    : 0
FcFecRxBlocksUncorrectedError  : 0
FcFecRxBlocksCorrectedErrorBits : 0
FcFecRxBlocksCorrectedError0   : 0
FcFecRxBlocksCorrectedError1   : 0
FcFecRxBlocksCorrectedError2   : 0
FcFecRxBlocksCorrectedError3   : 0
FcFecRxBlocksUncorrectedError0 : 0
FcFecRxBlocksUncorrectedError1 : 0
FcFecRxBlocksUncorrectedError2 : 0
FcFecRxBlocksUncorrectedError3 : 0
```

次の CLI は、イーサネット 1/14 ポートに一致する SFP-FEC カウンタに関する詳細情報を表示します。

```
firepower-4225(local-mgmt)# show portmanager counters ethernet 1 14
  Good Octets Received      : 2153
  Bad Octets Received      : 0
  MAC Transmit Error       : 0
  Good Packets Received    : 13
  Bad packets Received     : 0
  BRDC Packets Received    : 0
  MC Packets Received      : 13
  .....
  .....
  txqFilterDisc            : 0
  linkchange               : 1
  RsFeccorrectedFecCodeword : 0
  RsFecuncorrectedFecCodeword : 10
  RsFecsymbolError0       : 5
  RsFecsymbolError1       : 0
  RsFecsymbolError2       : 0
  RsFecsymbolError3       : 0
```

次の CLI は、イーサネット 1/5 ポートに一致するデジタル オプティカル モニタリング (DOM) 情報に関する詳細情報を表示します。

```
firepower-4245(local-mgmt)# show portmanager port-info ethernet 1 5
  ....
  ....
  DOM info:
  =====:

  Status/Control Register: 0800
    RX_LOS State: 0
    TX_FAULT State: 0
  Alarm Status: 0000
  No active alarms
  Warning Status: 0000
  No active warnings

  THRESHOLDS
  alarm
  -05.000
  002.9700
  001.0000
  001.0000
  000.5370

  high alarm
  high warning
  low warning
  low

  Temperature C +075.000 +070.000 +000.000
  Voltage V 003.6300 003.4650 003.1350
  Bias Current mA 012.0000 011.5000 002.0000
  Transmit power mW 034.6740 017.3780 002.5120
  Receive power mW 034.6740 017.3780 001.3490

  Environmental Information - raw values
  Temperature: 38.84 C
  Supply voltage: 33703 in units of 100uVolt
  Tx bias: 3499 in units of 2uAmp
  Tx power: 0.1 dBm (10251 in units of 0.1 uW)
  Rx power: -0.9 dBm (8153 in units of 0.1 uW)
  DOM (256 bytes of raw data in hex)
  =====
  0x0000 : 4b 00 fb 00 46 00 00 00 8d cc 74 04 87 5a 7a 76
```

```

0x0010 : 17 70 01 f4 16 76 03 e8 87 72 03 e8 43 e2 09 d0
0x0020 : 87 72 02 19 43 e2 05 45 00 00 00 00 00 00 00 00
0x0030 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0040 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0050 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 86
0x0060 : 26 54 83 a7 0d ab 28 0b 1f d9 00 00 00 00 08 00
0x0070 : 00 00 03 00 00 00 00 00 08 f3 00 00 00 00 00 01
0x0080 : 49 4e 55 49 41 43 53 45 41 41 31 30 2d 33 33 38
0x0090 : 38 2d 30 31 56 30 31 20 01 00 46 00 00 00 00 e3
0x00a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00c0 : 53 46 50 2d 31 30 2f 32 35 47 2d 43 53 52 2d 53
0x00d0 : 20 20 20 20 30 38 00 00 00 00 00 00 00 00 00 d1
0x00e0 : 1e 20 2a 2a 31 34 29 36 00 00 00 00 00 00 00 00
0x00f0 : 00 00 00 00 00 56 00 00 ff ff ff ff 00 00 00 cf
=====

```

PHY Data:

PAGE	IFC	OFFSET	VALUE	PAGE	IFC	OFFSET	VALUE
----	---	-----	-----	----	---	-----	-----

次の CLI は、パケットキャプチャのパラメータ設定に関する詳細情報を表示します。

```

firepower-4225(local-mgmt)# show portmanager switch pktcap-rules software
Software DB rule:1
Slot= 1
Interface= 12
Breakout-port= 0
Protocol= 6
Ethertype= 0x0000
Filter_key= 0x00000040
Session= 1
Vlan= 0
SrcPort= 0
DstPort= 0
SrcIp= 0.0.0.0
DstIp= 0.0.0.0
SrcIpv6= ::
DestIpv6= ::
SrcMacAddr= 00:00:00:00:00:00
DestMacAddr= 00:00:00:00:00:00

```

次の CLI は、FXOS ポートマネージャスイッチのハードウェア TCAM ルールに関する詳細情報を表示します。

```

firepower-4225(local-mgmt)# show portmanager switch pktcap-rules hardware
Hardware DB rule:1
Hw_index= 15372
Rule_id= 10241
Cnc_index= 1
Packet_count= 0
Slot= 1
Interface= 12
Protocol= 6
Ethertype= 0x0000
Vlan= 0
SrcPort= 0
DstPort= 0
SrcIp= 0.0.0.0
DstIp= 0.0.0.0
SrcIpv6= ::
DestIpv6= ::
SrcMacAddr= 00:00:00:00:00:00
DestMacAddr= 00:00:00:00:00:00

```

次の CLI は、8つのトラフィッククラス/キューのポートベースのパケットドロップに関する詳細情報を表示します。

```
firepower-4225(local-mgmt)# show portmanager switch tail-drop-allocated buffers all
```

Per Port and Traffic Class									
Port	Per port	TC0	TC1	TC2	TC3	TC4	TC5	TC6	TC7
0/1	10	10	0	0	0	0	0	0	0
0/2	15	5	5	5	0	0	0	0	0
0/3	0	0	0	0	0	0	0	0	0
0/4	80	0	0	0	0	0	0	0	0
0/5	0	0	0	0	0	0	0	0	0
0/6	0	0	0	0	0	0	0	0	0
0/7	200	25	25	50	0	0	25	50	0
0/8	0	0	0	0	0	0	0	0	0

次の CLI は、tti-lookup0 が原因でドロップされたパケット数を表示します。

```
firepower-4225(local-mgmt)# show portmanager switch default-rule-drop-counter tti-lookup0
```

Rule_id	cnc_index	packet_count
1	1	4

FXOS CLI セキュリティ サービス モード トラブルシューティング コマンド

システムに関する問題をトラブルシューティングするには、以下のセキュリティサービス (ssa) モード FXOS CLI コマンドを使用します。

show app

Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスに接続されているアプリケーションに関する情報を表示します。

次に例を示します。

```
firepower /ssa # show app
Application:
  Name      Version  Description Author      Deploy Type CSP Type  Is Defa
ult App
```

```

-----
-----
ftd          6.2.0.131  N/A          cisco        Native       Application No
ftd          6.2.0.140  N/A          cisco        Native       Application No
ftd          6.2.0.175  N/A          cisco        Native       Application Yes

```

showapp-instance

検証済みのアプリ インスタンス ステータスに関する情報を表示します。

```

firepower-2120 /ssa # show app-instance
Application Name      Slot ID   Admin State      Operational State      Running Version
Startup Version Cluster Oper State
-----
asa                  1         Enabled          Online                  9.14.2
9.14.2              Not Applicable

```

showfault

障害メッセージの情報を表示します。

```

firepower-2120 /ssa # show fault
Severity  Code      Last Transition Time      ID      Description
-----
Cleared   F16589    2021-10-11T21:58:53.200    25140   [FSM:STAGE:RETRY]: Waiting for
chassis object ready(FSM-STAGE:sam:dme:SmSecSvcAutoDeployCSP:WaitForChassisM
oReady)

```

show failsafe-params

Firepower 1000/2100 または Cisco Secure Firewall 3100 の Threat Defense アプリケーションのフェールセーフモードが、継続的な起動ループ、トレースバックなどのためにアクティブ化されます。次のパラメータは、フェールセーフモードのアクティブ化を制御します。

- **Max Restart** - フェールセーフモードをアクティブにするためにアプリケーションを再起動する必要がある最大回数。
- **Current Reboot Count** - アプリケーションが継続的に再起動された回数。
- **Restart Time Interval (secs)** - フェールセーフモードを起動するために Max Restart カウンタに到達するための時間 (秒単位)。アプリケーションがこの間隔内に「Max Restart」以上の回数再起動すると、フェールセーフモードが有効になります。

次に例を示します。

```

firepower-2120-failed(local-mgmt)# show failsafe-params
Max Restart: 8
Current Reboot Count: 0
Restart Time Interval(secs): 3600

```

システムがフェールセーフモードの場合：

- システム名に「-failed」文字列が追加されます。

```
firepower-2120-failed /ssa #
```

- **local-mgmt** コマンドシェルの「show failsafe-params」コマンドの出力には、次の警告メッセージが含まれます。

```

firepower-2120-failed(local-mgmt)# show failsafe-params
Max Restart: 1
Current Reboot Count: 1

```

```
Restart Time Interval(secs): 3600
WARNING: System in Failsafe mode. Applications are not running!
```

- アプリケーションの動作状態はオフラインです。

```
firepower-2120-failed /ssa # show app-instance
Application Name      Slot ID      Admin State      Operational State      Running Version
Startup Version Cluster Oper State      Cluster Role
-----
asa                   1           Enabled          Offline <=====      9.16.2.3
9.16.2.3              Not Applicable      None
```

Cisco Secure Firewall 1200/3100/4200 CLI モニタリングモードのトラブルシューティング コマンド

問題のトラブルシューティングを行うには、次の CLI コマンドを使用します。

show

プロセスに関するメモリリークの状態を表示します。
次に例を示します。

```
FPR3100 /monitoring/sysdebug/mem-leak-logging # show detail
Process      Status      Stacktrace
-----
statsAG      Disabled    Off
dcosAG       Disabled    Off
portAG       Disabled    Off
appAG        Disabled    Off
eventAG      Disabled    Off
npuAG        Disabled    Off
sessionmgrAG Disabled    Off
svcmonAG     Disabled    Off
serviceOrchAG Disabled    Off
dme          Disabled    Off
envAG        Disabled    Off
```



- (注) デフォルトでは、すべての UCSM プロセスに対して **mem-leak** が無効になっており、スタックトレースが無効になっています。メモリリークの問題をデバッグするには、指定されたプロセスに対して **mem-leak** を有効にし、問題の詳細についてはスタックトレースを有効にする必要があります。

Cisco Secure Firewall 3100/4200 のパケットキャプチャ

パケットキャプチャツールは、接続と設定に関する問題のデバッグや、デバイスを通過するトラフィックフローを理解する際に使用できる価値ある資産です。パケットキャプチャ CLI を使用して、Cisco Secure Firewall 3100/4200 デバイスの特定のインターフェイスを通過するトラフィックについてログを記録できるようになりました。

複数のパケット キャプチャ セッションを作成でき、各セッションで複数のインターフェイスのトラフィックをキャプチャできます。パケット キャプチャ セッションに含まれる各インターフェイス用に、個別のパケット キャプチャ (PCAP) ファイルが作成されます。

パケット キャプチャの注意事項および制限事項

パケット キャプチャ ツールには、次の制限事項があります。

- Cisco Secure Firewall 3100/4200 シリーズデバイスでのパケット キャプチャは、最大 300 Mbps まで可能です。
 - パケット キャプチャ セッションの使用に使用可能な十分な記憶域がなくても、パケット キャプチャ セッションを作成できます。パケット キャプチャ セッションを開始する前に、使用可能な十分な記憶域があることを確認する必要があります。
 - シングル幅の 4x100Gbps または 2x100Gbps ネットワーク モジュール (それぞれ部品番号 FPR-NM-4X100G および FPR-NM-2X100G) でのパケット キャプチャ セッションの場合、モジュールの `adminstate` が `off` に設定されると、キャプチャ セッションが自動的に無効になり、「Oper State Reason: Unknown Error」というメッセージが生成されます。モジュールの `adminstate` を再度 `on` に設定してから、キャプチャ セッションを再起動する必要があります。
- 他のすべてのネットワーク モジュールでは、モジュールの `adminstate` が変更されてもパケット キャプチャ セッションが継続されます。
- 複数のアクティブなパケット キャプチャ セッションはサポートされません。
 - 送信元または宛先 IPv6 アドレスに基づいてフィルタするオプションはありません。
 - 内部スイッチが認識できないパケット (セキュリティ グループ タグ、ネットワーク サービス ヘッダー パケットなど) にはフィルタの効果がありません。
 - EtherChannel 全体のパケットをキャプチャできません。ただし、論理デバイスに割り当てられている EtherChannel の場合、EtherChannel のメンバーインターフェイスごとにパケットをキャプチャできます。
 - キャプチャ セッションがアクティブな間は、PCAP ファイルをコピーしたり、エクスポートできません。
 - パケット キャプチャ セッションを削除すると、そのセッションに関連するすべてのパケット キャプチャ ファイルも削除されます。

パケット キャプチャ セッションの作成または編集

手順

ステップ 1 パケット キャプチャ モードを開始します。

```
firepower-4215 # scope packet-capture
```

ステップ 2 フィルタを作成します。

```
firepower-4215 /packet-capture/filter* # set <filterprop filterprop_value
```

表 2: サポートされるフィルタ プロパティ

ivlan	内部 VLAN ID (ポート入力時のパケットの VLAN)
ovlan	外部VLAN ID
srcip	送信元 IP アドレス (IPv4)
destip	宛先 IP アドレス (IPv4)
srcport	送信元ポート番号
destport	宛先ポート番号
protocol	IP プロトコル (IANA によって定義される 10 進形式のプロトコル値)
ethertype	イーサネットプロトコルタイプ (IANA によって定義される 10 進形式のイーサネットプロトコルタイプ値。たとえば、IPv4 = 2048、IPv6 = 34525、ARP = 2054、SGT = 35081)
srcmac	送信元 MAC アドレス
destmac	宛先 MAC アドレス

パケットキャプチャセッションに含まれるインターフェイスのいずれかにフィルタを適用できます。

ステップ 3 パケットキャプチャセッションを作成または編集するには、次の操作を行います。

```
firepower-4215 /packet-capture # enter session session_name
```

ステップ 4 このパケットキャプチャセッションでキャプチャするパケットの長さを指定します。

```
firepower-4215 /packet-capture/session* # set session-pcap-snaplength session_snap_length_in_bytes
```

スナップの指定長は、64 ~ 9006 バイトの範囲内にする必要があります。セッションスナップ長を設定しない場合のデフォルトのキャプチャ長は、1518 バイトです。

ステップ 5 このパケットキャプチャセッションに含める必要がある物理ソース ポートを指定します。

複数のポートからキャプチャしたり、物理ポートやアプリケーションポートの両方から同じパケットキャプチャセッション中に取得することができます。別のパケットキャプチャファイルがセッションに含まれる各ポート用に作成されます。EtherChannel 全体のパケットをキャプチャすることはできません。ただし、論理デバイスに割り当てられている EtherChannel の場合、EtherChannel のメンバー インターフェイスごとにパケットをキャプチャできます。

(注)

パケット キャプチャ セッションからポートを削除するには、次に示すコマンドで **create** の代わりに **delete** を使用します。

- a) 物理ポートを指定します。

```
firepower-4215 /packet-capture/session* # create {phy-port | phy-aggr-port} port_id
```

例 :

例 :

```
firepower-4215 /packet-capture/session* # create phy-port Ethernet1/1
firepower-4215 /packet-capture/session/phy-port* #
```

- b) サブインターフェイスのパケットをキャプチャします。

```
firepower-4215 /packet-capture/session/phy-port* # set subinterface id
```

1 つ以上の親で複数のサブインターフェイスを使用する場合でも、キャプチャセッションごとに 1 つのサブインターフェイスのパケットのみをキャプチャできます。Etherchannel のサブインターフェイスはサポートされていません。親インターフェイスをインスタンスにも割り当てる場合、親インターフェイスまたはサブインターフェイスのいずれかを選択できます。両方を選択することはできません。

例 :

```
firepower-4215 /packet-capture/session/phy-port* # set subinterface 100
firepower-4215 /packet-capture/session/phy-port* #
```

- c) コンテナ インスタンスの場合、コンテナ インスタンス名を指定します。

```
firepower-4215 /packet-capture/session/phy-port* # set app-identifier instance_name
```

例 :

```
firepower-4215 /packet-capture/session/phy-port* # set app-identifier ftd-instance1
firepower-4215 /packet-capture/session/phy-port* #
```

- d) (任意) スイッチから **mac-filter** ドロップパケットをキャプチャするには、**mac-filter** ドロップを指定します。

```
firepower-4215 /packet-capture/session/phy-port* # set drop {mac-filter | disable}
```

- **disable** : スイッチからドロップされたパケットのキャプチャを無効にします。
- **mac-filter** : スイッチの **mac-filter** ドロップをキャプチャします。

(注)

mac-filter オプションは、入力パケットキャプチャ方向でのみサポートされます。デフォルトのオプションは常に **disable** です。

- e) (任意) 目的のフィルタを適用します。

```
firepower-4215 /packet-capture/session/phy-port* # set {source-filter} filtername
```

(注)

ポートからフィルタを削除するには、**set source-filter ""** を使用します。

- f) 必要に応じて上記のステップを繰り返して必要なポートをすべて追加します。

ステップ 6 このパケット キャプチャ セッションに含める必要があるアプリケーション ソース ポートを指定します。

複数のポートからキャプチャしたり、物理ポートやアプリケーションポートの両方から同じパケット キャプチャ セッション中に取得することができます。別のパケット キャプチャ ファイルがセッションに含まれる各ポート用に作成されます。

(注)
パケット キャプチャ セッションからポートを削除するには、次に示すコマンドで **create** の代わりに **delete** を使用します。

- a) アプリケーション ポートを指定します。

```
firepower-4215 /packet-capture/session* # create app_port module_slot link_name interface_name app_name
```

構文の説明

module_slot	アプリケーションがインストールされているセキュリティモジュール。
link_name	インターフェイスを指すユーザー記述名 (link1、inside_port1 など)。
interface_name	パケットをキャプチャする必要があるアプリケーションに接続されているインターフェイス (Ethernet1/1、Ethernet2/2 など)。
app_name	モジュールにインストールされているアプリケーション (ftd)

- b) (任意) 目的のフィルタを適用します。

```
firepower-4215 /packet-capture/session/phy-port* # set {source-filter} filtername
```

構文の説明

filtername	「create filter」 コマンドによる packet-capture 範囲のフィルタ名。
-------------------	--

(注)
ポートからフィルタを削除するには、**set source-filter ""** を使用します。

- c) 必要に応じて上記のステップを繰り返して必要なアプリケーションポートをすべて追加します。

ステップ 7 パケット キャプチャ セッションをすぐに開始するには、次の操作を行います。

```
firepower-4215 /packet-capture/session* # enable
```

新しく作成したパケット キャプチャ セッションはデフォルトでは無効になっています。セッションを明示的に有効にすると、変更がコミットされたときにパケット キャプチャ セッションがアクティブになります。別のセッションがすでにアクティブになっている場合、セッション

ンを有効にするとエラーが生成されます。このセッションを有効にする前に、すでにアクティブなパケットキャプチャセッションを無効にする必要があります。

ステップ 8 トランザクションをシステム設定にコミットします。

```
firepower-4215 /packet-capture/session* # commit-buffer
```

パケットキャプチャセッションを有効にすると、システムはパケットのキャプチャを開始します。セッションからPCAPファイルをダウンロードする前に、キャプチャを停止する必要があります。

例

```
firepower-4215 # scope packet-capture
firepower-4215 /packet-capture # create session ftdlinside
firepower-4215 /packet-capture* # create filter interfacelvlan100
firepower-4215 /packet-capture/filter* # set ivlan 100
firepower-4215 /packet-capture/filter* # set srcIP 6.6.6.6
firepower-4215 /packet-capture/filter* # set destIP 10.10.10.10
firepower-4215 /packet-capture/filter* # exit
firepower-4215 /packet-capture/session* # create phy-port Ethernet1/1
firepower-4215 /packet-capture/session/phy-port* # set drop mac-filter
firepower-4215 /packet-capture/session/phy-port* # set src-filter interfacelvlan100
firepower-4215 /packet-capture/session/phy-port* # exit
firepower-4215 /packet-capture/session* # enable
firepower-4215 /packet-capture/session* # commit-buffer
firepower-4215 /packet-capture/session #
```

パケットキャプチャセッションの削除

個々のパケットキャプチャセッションは、現在実行していなければ削除できます。非アクティブパケットキャプチャセッションは、いずれも削除できます。

手順

ステップ 1 パケットキャプチャモードを開始します。

```
firepower-4215 # scope packet-capture
```

ステップ 2 特定のパケットキャプチャセッションを削除するには、次の手順を実行します。

```
firepower-4215 /packet-capture # delete session session_name
```

ステップ 3 すべての非アクティブパケットキャプチャセッションを削除するには、次のようにします。

```
firepower-4215 /packet-capture # delete-all-sessions
```

ステップ 4 トランザクションをシステム設定にコミットします。

```
firepower-4215 /packet-capture* # commit-buffer
```

例

```
firepower-4215 # scope packet-capture  
firepower-4215 packet-capture # delete session asalinside  
firepower-4215 packet-capture* # commit-buffer  
firepower-4215 packet-capture #
```



第 4 章

イメージ管理

- ディザスタリカバリの概要 (49 ページ)
- ベース インストール ソフトウェア バージョンを使用したシステムの再イメージ化 (50 ページ)
- **ROMMON** からの工場出荷時設定へのリセットの実行 (パスワードのリセット) (53 ページ)
- 新しいソフトウェアバージョンを使用したシステムの再イメージ化 (55 ページ)
- マルチインスタンスモードのパッケージのダウンロード (59 ページ)
- **SSD** ファイルシステムの再フォーマット (Firepower 2100) (60 ページ)
- **ROMMON** からの起動 (60 ページ)
- 完全な再イメージ化の実行 (68 ページ)
- 管理者パスワードの変更 (73 ページ)
- **Threat Defense** がオフラインの場合の管理者パスワードの変更 (74 ページ)
- クラウドからの登録解除 (75 ページ)
- **Firepower 1000/2100** および **Cisco Secure Firewall 3100/4200 FXOS** トラブルシューティングの履歴 (77 ページ)

ディザスタリカバリの概要

設定のリセット、イメージの再インストール、FXOS パスワードの回復、またはシステムの完全な再イメージ化が必要になる場合があります。次の該当する手順を参照してください。

- 設定の消去と同じイメージでのシステムの再起動：すべての設定が削除され、現在のイメージを使用して **Threat Defense** が再インストールされます。この手順を実行する場合は、実行後に、管理者パスワードや接続情報などを含めて、システムを再設定する必要があります。ベース インストール ソフトウェア バージョンを使用したシステムの再イメージ化 (50 ページ) を参照してください。
- **ROMMON** からの工場出荷時設定へのリセットの実行 (管理者パスワードの回復)：すべての設定が削除され、現在のイメージを使用して **Threat Defense** が再インストールされます。この手順を実行する場合は、実行後に、管理者パスワードや接続情報などを含めて、

システムを再設定する必要があります。[ROMMON からの工場出荷時設定へのリセットの実行（パスワードのリセット）（53 ページ）](#)を参照してください。

- 新しいバージョンでのシステムの再イメージ化：すべての設定が削除され、新しいソフトウェアイメージを使用して Threat Defense が再インストールされます。この手順を実行する場合は、実行後に、管理者パスワードや接続情報などを含めて、システムを再設定する必要があります。[新しいソフトウェアバージョンを使用したシステムの再イメージ化（55 ページ）](#)を参照してください。



(注) この手順を使用して以前のメジャーバージョンにダウングレードすることはできません。代わりに[完全な再イメージ化の実行（68 ページ）](#)を使用する必要があります。

- SSD ファイルシステムの再フォーマット：ディスク破損メッセージが表示された場合に SSD を再フォーマットします。すべての設定が削除されます。この手順を実行する場合は、実行後に、管理者パスワードや接続情報などを含めて、システムを再設定する必要があります。[SSD ファイルシステムの再フォーマット（Firepower 2100）（60 ページ）](#)を参照してください。
- ROMMON からの起動：FXOS を起動できない場合に ROMMON から起動します。その後、eMMC を再フォーマットし、ソフトウェアイメージを再インストールできます。この手順では、すべての設定が保持されます。[ROMMON からの起動（60 ページ）](#)を参照してください。
- すべての設定とイメージの消去：システムを工場出荷時のデフォルト設定に戻し、イメージを消去します。この手順では、TFTP 経由でシステムを起動し、Threat Defense ソフトウェアをダウンロードし、システム全体を再設定する必要があります。[完全な再イメージ化の実行（68 ページ）](#)を参照してください。
- 管理者パスワードの変更：Threat Defense CLI から管理者パスワードを変更します。[管理者パスワードの変更（73 ページ）](#)を参照してください。
- Threat Defense がオフラインの場合の管理者パスワードの変更：FXOS から管理者パスワードを変更します。[Threat Defense がオフラインの場合の管理者パスワードの変更（74 ページ）](#)を参照してください。Threat Defense がオンラインの場合は、Threat Defense CLI を使用して管理者パスワードを変更する必要があります。

ベース インストール ソフトウェア バージョンを使用したシステムの再イメージ化

この手順を実行すると、ベース インストール ソフトウェア バージョンの設定を除き、すべての設定が消去されます。設定の消去操作後にシステムが再起動すると、Threat Defense のスタートアップバージョンが実行されます。

現在実行中のバージョンがアップグレード専用イメージの場合は、この手順を実行した後、Threat Defense を再アップグレードする必要があります。たとえば、バージョン 6.2.2.x はアップグレード専用のイメージです。6.2.2.x システムでこの手順を実行すると、ベースインストールパッケージ（バージョン 6.2.1.x）が再インストールされます。その後、Secure Firewall Management Center または Secure Firewall Device Manager を使用してバージョン 6.2.2.x に再アップグレードする必要があります。この場合、FXOS のバージョンが下位バージョンに戻らないことがあります。この不一致により、ハイアベイラビリティ構成で障害が発生する可能性があります。このシナリオでは、システムの完全な再イメージ化を実行することを推奨します（詳細については、[完全な再イメージ化の実行（68 ページ）](#)を参照してください）。



(注) この手順を実行すると、管理者パスワードが **Admin123** にリセットされます。

始める前に

- FXOS CLI コンテキストに接続されていることを確認します。シリアルコンソールを介して Firepower 1000/2100、Cisco Secure Firewall 1200、3100、4200 デバイスに接続すると、FXOS CLI コンテキストに自動的に接続されます。Threat Defense CLI コンテキストに接続されている場合は、まず **connect fxos** コマンドを使用して FXOS CLI コンテキストに切り替える必要があります。
- アプライアンスの管理 IP アドレスの設定をメモし、次のコマンドで示される情報をコピーします。

```
firepower # scope fabric a
firepower /fabric-interconnect # show detail
```

- 次のコマンドを使用して Threat Defense のベース インストール バージョンを確認し、メモしておきます。起動バージョンの列には、ベース インストール バージョンが表示されます。「Running Version」には、ベース インストールバージョンに適用したアップグレードが表示されます。

```
firepower# scope ssa
firepower /ssa # show app-instance
Application Name      Slot ID   Admin State      Operational State      Running Version
Startup Version Cluster Oper State
-----
ftd                    1         Enabled          Online                  6.2.2.49
6.2.1.341              Not Applicable
```

- Smart Licensing からデバイスの関連付けを解除します。
- クラウドテナントからデバイスを登録解除します（該当する場合）。[クラウドからの登録解除（75 ページ）](#)を参照してください。
- Cisco Secure Firewall 3100 デバイスを Threat Defense 7.3.0 バージョンに再イメージ化するには、ROMMON バージョン 1.1.08 以降が必要です。現在の ROMMON バージョンが 1.1.08

未満の場合は、ASA 9.19 以降にアップグレードして ROMMON をアップグレードする必要があります。Management Center または Device Manager を使用して Threat Defense を 7.3.0 にアップグレードすることもできます（詳細については、[Threat Defense Reimage](#) を参照してください）。

- Threat Defense イメージのインストールとアップグレードに単一イメージが導入されているため、ベース インストール ソフトウェア バージョンを使用して Cisco Secure Firewall 3100 デバイスを Threat Defense 7.4 に再イメージ化することはできません。代わりに、システムの完全な再イメージ化を実行します。詳細については、[完全な再イメージ化の実行 \(68 ページ\)](#) を参照してください。

手順

ステップ 1 FXOS CLI でローカル管理に接続します。

```
firepower # connect local-mgmt
```

ステップ 2 すべての設定を消去します。

```
firepower(local-mgmt) # erase configuration
```

例：

```
firepower(local-mgmt)# erase configuration
All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
Removing all the configuration. Please wait....
Configurations are cleaned up. Rebooting....
```

ステップ 3 システムが再起動したら、**show app-instance** コマンドを使用してアプリケーションの状態を確認できます。パスワードログインは、デフォルトの **admin/Admin123** にリセットされます。

例：

```
firepower# scope ssa

firepower /ssa # show app-instance
Application Name      Slot ID   Admin State      Operational State      Running Version
Startup Version Cluster Oper State
-----
ftd                   1         Disabled         Installing
6.2.1-1314           Not Applicable
```

(注)

アプリケーションのインストールが完了するまで 10 分以上かかります。Threat Defense がオンライン状態に戻ると、**show app-instance** コマンドの Operational State に「Online」と表示されます。

例：

```
firepower /ssa # show app-instance
Application Name      Slot ID   Admin State      Operational State      Running Version
Startup Version Cluster Oper State
-----
```



```
-----
ftd                        1                        Enabled                Online                6.2.1.10140
```

次のタスク

スタートアップガイドのセットアップタスクを完了し、必要に応じて最新バージョンにアップグレードします。

ROMMON からの工場出荷時設定へのリセットの実行（パスワードのリセット）

FXOS にログインできない場合（パスワードを忘れた場合、または SSD disk1 ファイルシステムが破損している場合）は、ROMMON を使用して FXOS および Threat Defense の設定を工場出荷時のデフォルトに復元できます。管理者パスワードはデフォルトの **Admin123** にリセットされます。パスワードがわかっていて、FXOS 内から工場出荷時のデフォルト設定を復元する場合は、[ベース インストール ソフトウェア バージョンを使用したシステムの再イメージ化（50 ページ）](#) を参照してください。

始める前に

- Cisco Secure Firewall 3100 デバイスを Threat Defense 7.3.0 バージョンに再イメージ化するには、ROMMON バージョン 1.1.08 以降が必要です。現在の ROMMON バージョンが 1.1.08 未満の場合は、ASA 9.19 以降にアップグレードして ROMMON をアップグレードする必要があります。Management Center または Device Manager を使用して、Threat Defense のバージョンを 7.3.0 にアップグレードすることもできます（詳細については、[Threat Defense Reimage](#) を参照してください）。

手順

ステップ 1 デバイスの電源を入れます。次のようなプロンプトが表示されたら、ESC キーを押してブートを中断します。

```
Example:
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

ステップ 2 ROMMON のバージョンを確認します。

```
rommon 1 > show info
```

例：

Firepower 1000 および 2100 デバイス

```
rommon 1 > show info
```

```
Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
Copyright (c) 1994-2017 by Cisco Systems, Inc.
Compiled Wed 11/01/2017 18:38:59.66 by builder
```

Cisco Secure Firewall 3100 デバイス

```
rommon 1 > show info
Cisco System ROMMON, Version 1.1.08 , RELEASE SOFTWARE
Copyright (c) 1994-2022 by Cisco Systems, Inc.
Compiled Fri 06/10/2022 10:25:43.78 by Administrator
```

Cisco Secure Firewall 4200 デバイス

```
Cisco System ROMMON, Version 1.0.15, RELEASE SOFTWARE
Copyright (c) 1994-2023 by Cisco Systems, Inc.
Compiled Thu 06/15/2023 14:41:54.43 by builder
```

ステップ3 デバイスを工場出荷時設定にリセットします。

ROMMON バージョン1.0.06 以降の場合：

```
rommon 2 > factory-reset
```

ROMMON バージョン1.0.04 の場合：

```
rommon 2 > password_reset
```

例：

Firepower 1000 および 2100 デバイス

```
rommon 2 > factory-reset
Warning: All configuration will be permanently lost with this operation
and application will be initialized to default configuration.
This operation cannot be undone after booting the application image.

Are you sure you would like to continue ? yes/no [no]: yes
Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE

Performing factory reset...
File size is 0x0000001b
Located .boot_string
Image size 27 inode num 16, bks cnt 1 blk size 8*512

Rommon will continue to boot disk0: fxos-k8-fp2k-lfbff.2.3.1.132.SSB
Are you sure you would like to continue ? yes/no [no]: yes
File size is 0x0817a870
Located fxos-k8-fp2k-lfbff.2.3.1.132.SSB
```

例：

Cisco Secure Firewall 3100 デバイス

```
rommon 2 > factory-reset
Warning: All configuration will be permanently lost with this operation
and application will be initialized to default configuration.
This operation cannot be undone after booting the application image.

Are you sure you would like to continue ? yes/no [no]: yes
Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE

Performing factory reset...
File size is 0x0000001b
Located .boot_string
```

```
Image size 27 inode num 16, bks cnt 1 blk size 8*512
```

```
Rommon will continue to boot disk0: Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
Are you sure you would like to continue ? yes/no [no]: yes
File size is 0x0817a870
Located Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
```

例：

Cisco Secure Firewall 4200 デバイス

```
rommon 2 > factory-reset
Warning: All configuration will be permanently lost with this operation
        and application will be initialized to default configuration.
        This operation cannot be undone after booting the application image.

Are you sure you would like to continue ? yes/no [no]: yes
Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE
```

```
Performing factory reset...
File size is 0x0000001b
Located .boot_string
Image size 27 inode num 16, bks cnt 1 blk size 8*512
```

```
Rommon will continue to boot disk0: Cisco_Secure_FW_TD_4200-7.4.0-1044.sh.DEV.tar
Are you sure you would like to continue ? yes/no [no]: yes
File size is 0x0817a870
Located Cisco_Secure_FW_TD_4200-7.4.0-1044.sh.DEV.tar
```

ステップ 4 システムから起動を求めるプロンプトが表示されない場合は、**boot** コマンドを入力します。

```
rommon 3 > boot
```

次のタスク

スタートアップガイドのセットアップタスクを実行します。

新しいソフトウェアバージョンを使用したシステムの再イメージ化

この手順では、新しいソフトウェアバージョンでシステムを再イメージ化できます。この手順を実行した後、デバイスの管理 IP アドレスとその他の設定パラメータを再設定する必要があります。設定を消去せずにソフトウェアをアップグレードする場合は、アップグレードガイドを参照してください。



(注) この手順を使用して以前のメジャーバージョンにダウングレードすることはできません。代わりに [完全な再イメージ化の実行 \(68 ページ\)](#) を使用する必要があります。



(注) この手順を実行すると、管理者パスワードが **Admin123** にリセットされます。

始める前に

- FXOS CLI コンテキストに接続されていることを確認します。シリアルコンソールを介して Firepower 1000/2100、Cisco Secure Firewall 1200、3100、4200 デバイスに接続すると、FXOS CLI コンテキストに自動的に接続されます。Threat Defense CLI コンテキストに接続されている場合は、まず **connect fxos** コマンドを使用して FXOS CLI コンテキストに切り替える必要があります。
- アプライアンスの管理 IP アドレスの設定をメモし、次のコマンドで示される情報をコピーします。

```
firepower # scope fabric a
firepower /fabric-interconnect # show detail
```

- Smart Licensing からデバイスの関連付けを解除します。
- クラウドテナントからデバイスを登録解除します（該当する場合）。[クラウドからの登録解除（75 ページ）](#) を参照してください。
- Cisco Secure Firewall 3100 デバイスを Threat Defense バージョン 7.3.0 に再イメージ化するには、ROMMON バージョン 1.1.08 以降が必要です。現在の ROMMON バージョンが 1.1.08 未満の場合は、ASA 9.19 以降にアップグレードして ROMMON をアップグレードする必要があります。Management Center または Device Manager を使用して、Threat Defense のバージョンを 7.3.0 にアップグレードすることもできます（詳細については、[Threat Defense Reimage](#) を参照してください）。

手順

-
- ステップ 1** ソフトウェアバンドルをローカルコンピュータまたは USB フラッシュドライブにダウンロードします。
- ステップ 2** USB ドライブを使用する場合は、アプライアンスの USB ポートに USB ドライブを挿入します。
- ステップ 3** FXOS で、システムのスコープを入力し、システムで現在実行されているバージョンを確認します。
- ```
firepower # scope system
firepower /system # show version detail
```
- ステップ 4** ファームウェアのスコープを入力します。
- ```
firepower # scope firmware
```

- ステップ 5** 新しいソフトウェアパッケージをダウンロードします。USB ドライブを使用してソフトウェアパッケージをダウンロードする場合は、次の構文を使用します。

```
firepower # scope firmware
```

```
firepower /firmware # download image usbA:image_name
```

image_name は、ステップ 3（上記）の **show version detail** コマンドの出力です。

次に例を示します。

```
firepower /firmware # download image usbA:cisco-ftd-fp2k.6.2.1-36.SPA
```

（注）

バージョン 7.3+ では、Cisco Secure Firewall 3100 の Threat Defense のインストールおよびアップグレードパッケージを組み合わせたパッケージとなっています。説明されている手順では、.SPA ファイルの代わりに.REL.tar ファイルを使用できます。

FTP、SCP、SFTP、TFTP を使用して、Threat Defense ソフトウェアパッケージをデバイスにコピーすることもできます。

```
firepower /firmware # download image tftp/ftp/scp/sftp://path to the image, including the server root /image name
```

Firepower 1000 および 2100 デバイスの例を示します。

```
firepower /firmware # download image tftp://example.cisco.com/fxos-2k.6.2.1-1314.SPA
```

Cisco Secure Firewall 3100 デバイスの例を示します。

```
firepower /firmware # download image  
scp://example.cisco.com/auto/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar
```

Cisco Secure Firewall 4200 デバイスの例を示します。

```
firepower-4215 /firmware # download image tftp://172.29.185.101:/Cisco_Secure_FW_TD_4200-7.4.0-1044.sh.REL.tar
```

（注）

システムはダウンロードイメージ要求で指定されたファイル名の前にスラッシュを付加するので、FTP/TFTP/SCP/SFTP によりファイル転送を実行する場合は、サーバのルートを含むイメージの絶対パスを入力する必要があります。

必要に応じて、IP アドレスの代わりに FQDN を使用できます。

- ステップ 6** ダウンロードタスクを表示して、ダウンロードの進行状況をモニタします。

```
firepower /firmware # show download-task
```

Status 列の出力に「Downloaded」と表示されたら、ダウンロードは完了です。

例：

Cisco Secure Firewall 3100 デバイス

```
firepower 3110 /firmware # show download task
File Name Protocol Server Port Userid State
-----
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar
Scp 172.23.205.217 0 <xxxxxx> Downloaded
```

例：

Cisco Secure Firewall 4200 デバイス：

```
firepower-4215 /firmware # show download-task

Download task:
  File Name Protocol Server Port Userid State
  -----
  Cisco_Secure_FW_TD_4200-7.4.0-1044.sh.REL.tar
  Tftp 172.29.185.101 0 Downloading
```

ステップ 7 ダウンロードの完了後、システムにインストールされているソフトウェア パッケージを表示し、出力に示されているバンドル イメージバージョンをコピーします。

firepower /firmware # **show package**

例：

Firepower 1000 および 2100 デバイス

```
firepower /firmware # show package
Name Package-Vers
-----
cisco-ftd-fp2k.6.2.1-1314.SPA 6.2.1-1314
```

上記の例では、**6.2.1-1314** はセキュリティパックのバージョンです。

例：

Cisco Secure Firewall 3100 デバイス

```
firepower 3110 /firmware # show package
Name Package Vers
-----
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar 7.3.0-14
```

例：

Cisco Secure Firewall 4200 デバイス

```
firepower-4215 /firmware # show package
Name Package-Vers
-----
Cisco_Secure_FW_TD_4200-7.4.0-1044.sh.REL.tar 7.4.0-1044
```

上記の例では、**7.3.0-14** はセキュリティパックのバージョンです。

ステップ 8 自動インストールのスコープを入力します。

firepower /firmware # **scope auto-install**

ステップ 9 新しいアプリケーション ソフトウェア パッケージをインストールします（*version* は上記の `show package` の出力です）。

firepower /firmware/auto-install # **install security-pack version version**

例：

```
firepower 3110 /firmware/auto install # install security pack version 7.3.0-14
...
firepower /firmware # connect ftd
> show version
-----[ firepower 3100 ]-----
Model : Cisco Secure Firewall 3110 Threat Defense (80) Version 7.3.0 (Build
```

ステップ 10 入力を求められたら、**yes** と入力します。

システムが再起動し、最新のソフトウェアバンドルがインストールされます。

次のタスク

スタートアップガイドのセットアップタスクを実行します。

マルチインスタンスモードのパッケージのダウンロード

この手順では、古いThreat Defense パッケージをマルチインスタンスシャーシにダウンロードできるため、そのバージョンを使用してインスタンスを追加できます。FXOS イメージとThreat Defense イメージの両方が同じパッケージに含まれているため、シャーシの FXOS バージョンをアップグレードした場合でも、一致する古いThreat Defense バージョンを引き続きインスタンスで使用できます。

実行中の FXOS バージョンと互換性のないThreat Defense は使用できません。たとえば、最初にシャーシをアップグレードせずに新しいThreat Defense を使用することはできません。

始める前に

- FXOS CLI に接続されていることを確認します。コンソールからデバイスに接続すると、FXOS CLI に自動的に接続されます。デバイスに SSH 接続する場合は、Threat Defense CLI に接続し、**connect fxos** コマンドを使用して FXOS CLI にアクセスする必要があります。

手順

ステップ 1 FTP、SCP、SFTP、TFTP サーバー、または USB フラッシュドライブにパッケージをコピーします。

ステップ 2 USB ドライブを使用する場合は、デバイスの USB ポートに USB ドライブを挿入します。

ステップ 3 古いソフトウェアパッケージをダウンロードします。

```
firepower # scope firmware
```

```
firepower /firmware # download image url
```

例：

たとえば、USB ドライブ (usbA) からダウンロードするには、次のように入力します。

```
firepower-3110 /firmware # download image
usbA:Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-15.sh.DEV.tar
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
% Download-task Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-15.sh.DEV.tar : completed successfully.
```

たとえば、SCP サーバーからダウンロードするには、次のように入力します。

```
firepower-3110 /firmware # download image
scp://example.cisco.com/auto/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-78.sh.REL.tar
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
% Download-task Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-78.sh.DEV.tar : completed successfully.
```

ステップ 4 インスタンスを追加するときにパッケージを使用できるようになりました。

SSD ファイルシステムの再フォーマット (Firepower2100)

FXOS に正常にログインしたが、ディスク破損エラーメッセージが表示された場合は、FXOS および Threat Defense 設定が保存されている SSD1 を再フォーマットできます。この手順により、FXOS 設定が工場出荷時のデフォルトに復元されます。管理者パスワードはデフォルトの **Admin123** にリセットされます。この手順では、Threat Defense の設定もリセットされます。

この手順は Firepower 1000 および Cisco Secure Firewall 3100 に適用されません。このため、スタートアップイメージを維持しながら SSD を消去することはできません。

手順

ステップ 1 コンソールポートから FXOS CLI に接続します。

ステップ 2 SSD1 を再フォーマットします。

```
connect local-mgmt
```

```
format ssd1
```

ステップ 3 スタートアップガイドのセットアップタスクを実行します。

ROMMON からの起動

デバイスを起動できない場合は、TFTP サーバーまたは EXT2/3/4、VFAT/FAT32 形式の USB ドライブから FXOS を起動できる ROMMON が起動します。FXOS を起動した後、eMMC (ソ

フトウェアイメージを保持する内部フラッシュデバイス) を再フォーマットできます。再フォーマットした後、イメージを eMMC に再ダウンロードする必要があります。この手順では、個別の `ssd1` に保存されているすべての設定が保持されます。

電力障害やその他のまれな状態が原因で、eMMC ファイルシステムが破損している可能性があります。

始める前に

- この手順を実行するには、コンソールにアクセスする必要があります。
- Cisco Secure Firewall 3100 デバイスを Threat Defense バージョン 7.3.0 に再イメージ化するには、ROMMON バージョン 1.1.08 以降が必要です。現在の ROMMON バージョンが 1.1.08 未満の場合は、ASA 9.19 以降にアップグレードして ROMMON をアップグレードする必要があります。Management Center または Device Manager を使用して、Threat Defense のバージョンを 7.3.0 にアップグレードすることもできます (詳細については、[Threat Defense Reimage](#) を参照してください)。

手順

ステップ 1 起動できない場合、システムは ROMMON を起動します。ROMMON が自動的に起動されない場合、ブートアップ中に ROMMON プロンプトを表示するよう要求されたら、**Esc** を押します。モニタを注視します。

例：

```
*****
Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
Copyright (c) 1994-2018 by Cisco Systems, Inc.
Compiled Thu 04/06/2018 12:16:16.21 by builder
*****

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM_1/1 : Present
DIMM_2/1 : Present

Platform FPR-2130 with 32768 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 0c:75:bd:08:c9:80

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

この時点で、Esc を押します。

ステップ 2 USB ドライブ上のイメージから EXT2/3/4 または VFAT/FAT32 形式で起動するか、TFTP を使用してネットワークを介して起動します。

(注)

6.4以前の場合、ROMMONからFXOSを起動し、現在インストールされているイメージもブート可能である場合は、現在インストールされているイメージと同じバージョンを起動していることを確認してください。それ以外の場合、FXOS/Threat Defense バージョンが一致しないと、Threat Defense がクラッシュします。6.5以降では、ROMMONからFXOSを起動すると、Threat Defense が自動的にロードされなくなります。

USB から起動する場合は、次のようにします。

(注)

システムの稼動中に USB デバイスを挿入した場合、USB デバイスを認識させるにはシステムを再起動する必要があります。

boot usb:/path/filename

デバイスはFXOS CLIに起動します。ディスクの内容を表示するには、**dir usb:** コマンドを使用します。

例：

```
rommon 1 > dir usb:
rommon 2 > boot usb:/cisco-ftd-fp3k.7.1.0.SPA
```

TFTP から起動する場合は、次のようにします。

管理 1/1 のネットワーク設定を指定し、次の ROMMON コマンドを使用して Threat Defense パッケージをロードします。

address management_ip_address

netmask subnet_mask

server tftp_ip_address

gateway gateway_ip_address

filepath/filename

set

sync

tftpdnld -b

FXOS イメージがダウンロードされ、CLI にブートアップされます。

次の情報を参照してください。

- **set**：ネットワーク設定を表示します。**ping** コマンドを使用してサーバへの接続を確認することもできます。
- **sync**：ネットワーク設定を保存します。
- **tftpdnld -b**：FXOS をロードします。

例：

Firepower 1000 および 2100 デバイス

```

rommon 1 > address 10.86.118.4
rommon 2 > netmask 255.255.252.0
rommon 3 > server 10.86.118.21
rommon 4 > gateway 10.86.118.1
rommon 5 > file cisco-ftd-fp2k.6.4.0.SPA
rommon 6 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
  NETMASK=255.255.252.0
  GATEWAY=10.86.118.21
  SERVER=10.86.118.21
  IMAGE=cisco-ftd-fp2k.6.4.0.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7 > sync
rommon 8 > tftpdnld -b
Enable boot bundle: tftp_reqsize = 268435456

  ADDRESS: 10.86.118.4
  NETMASK: 255.255.252.0
  GATEWAY: 10.86.118.21
  SERVER: 10.86.118.1
  IMAGE: cisco-ftd-fp2k.6.4.0.SPA
  MACADDR: d4:2c:44:0c:26:00
  VERBOSITY: Progress
  RETRY: 40
  PKTTIMEOUT: 7200
  BLKSIZE: 1460
  CHECKSUM: Yes
  PORT: GbE/1
  PHYMODE: Auto Detect

link up
Receiving cisco-ftd-fp2k.6.4.0.SPA from 10.86.118.21!!!!!!!
[...]
```

サーバーへの接続をトラブルシューティングするには、Ping を実行します。

```

rommon 1 > ping 10.86.118.21
Sending 10, 32-byte ICMP Echoes to 10.86.118.21 timeout is 4 seconds
!!!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 2 >
```

例 :

Cisco Secure Firewall 3100 デバイス

```

rommon 1 > show info

Cisco System ROMMON, Version 1.1.08, RELEASE SOFTWARE
Copyright (c) 1994-2022 by Cisco Systems, Inc.
Compiled Fri 06/10/2022 10:25:43.78 by Administrator
*****

rommon 2 > ADDRESS=172.16.0.50
rommon 3 > NETMASK=255.255.255.0
rommon 4 > GATEWAY=172.16.0.254
rommon 5 > SERVER=172.23.37.186
rommon 6 > IMAGE=image_dir/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
```

```
rommon 7 > set
ADDRESS=172.16.0.50
NETMASK=255.255.255.0
GATEWAY=172.16.0.254
SPEED=10000
SERVER=172.23.37.186
IMAGE= image_dir/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
CONFIG=
PS1="rommon ! > "
FIRMWARE_VERSION=1.3.5

rommon 8 > sync
rommon 9 > tftpdnld -b
Enable boot bundle: tftp_reqsize = 402653184

ADDRESS: 172.16.0.50
NETMASK: 255.255.255.0
GATEWAY: 172.16.0.254
SERVER: 172.23.37.186
IMAGE: image_dir/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
VERBOSITY: Progress
RETRY: 40
PKTTIMEOUT: 7200
BLKSIZE: 1460
CHECKSUM: Yes
PORT: 10G/1
PHYMODE: Auto Detect

.=====
+-----+
+-----+ SUCCESS +-----+
+-----+
|
| LFBFF signature authentication passed !!!
|
+-----+
LFBFF signature verified.
```

ステップ 3 現在の管理者パスワードを使用して FXOS にログインします。

(注)

ログイン情報がわからない場合、またはディスクの破損が原因でログインできない場合は、ROMMON **factory-reset** コマンドを使用して工場出荷時設定へのリセットを実行する必要があります ([ROMMON からの工場出荷時設定へのリセットの実行 \(パスワードのリセット\)](#) (53 ページ) を参照)。初期設定へのリセットを実行したら、この手順を再開して FXOS を起動し、デフォルトのログイン情報 (**admin/Admin123**) でログインします。

ステップ 4 EMMC を再フォーマットします。

connect local-mgmt

format emmc

yes と入力します。

例 :

```
firepower-2110# connect local-mgmt
firepower-2110(local-mgmt)# format emmc
All bootable images will be lost.
Do you still want to format? (yes/no):yes
```

```
firepower-3110# connect local-mgmt
firepower-3110(local-mgmt)# format emmc
All bootable images will be lost.
Do you still want to format? (yes/no):yes
```

ステップ 5 サーバーからイメージをダウンロードできるように管理インターフェイスを設定します。

USB を使用する場合は、この手順をスキップできます。

- a) ファブリック インターコネクトのスコープを入力します。

scope fabric-interconnect a

- b) 新しい管理 IP 情報を設定します。

set out-of-band static ip ip netmask netmask gw gateway

- c) 設定をコミットします。

commit-buffer

例：

```
firepower# scope fabric-interconnect a
firepower /fabric-interconnect # set out-of-band static ip 10.1.1.5 netmask 255.255.255.0
gw 10.1.1.1
firepower /fabric-interconnect* # commit-buffer
```

(注)

次のエラーが発生する場合は、変更をコミットする前に DHCP を無効にする必要があります。
DHCP を無効にするには、次の手順に従います。

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask> ) is not
in the same network of current DHCP server IP range <ip - ip>].
Either disable DHCP server first or config with a different ipv4 address.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # commit-buffer
```

ステップ 6 Threat Defense パッケージを再ダウンロードして起動します。

- a) パッケージをダウンロードします。USB または TFTP から一時的に起動したので、引き続きローカルディスクにイメージをダウンロードする必要があります。

scope firmware

download image url

show download-task

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp://username@server/[path/]image_name**

- **scp://username@server/[path/]image_name**
- **sftp://username@server/[path/]image_name**
- **tftp://server[:port]/[path/]image_name**
- **usbA:/path/filename**

例：

Firepower 1000 および 2100 デバイス

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.86.118.21/cisco-asa-fp2k.9.8.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
firepower-2110 /firmware # show download-task
Download task:
  File Name Protocol Server Port Userid State
  -----
  cisco-asa-fp2k.9.8.2.SPA
                        Tftp 10.88.29.21 0 Downloaded
```

例：

Cisco Secure Firewall 3100 デバイス

```
firepower-3110# scope firmware
firepower-3110 /firmware # download image
scp://172.23.205.217/auto/Cisco_FTD_SSP_FP3K_Upgrade 7.3.0-14.sh.REL.tar
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
firepower-3110 /firmware # show download-task
Download task:
  File Name Protocol Server Port Userid State
  -----
  Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar 7.3.0-14.sh.REL.tar
                        Scp 172.23.205.217 0 Downloaded
```

- b) パッケージのダウンロードが完了 ([ダウンロード済み (Downloaded)] の状態) したら、パッケージを起動します。

show package

scope auto-install

install security-pack version version

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。
シャーンが ASA イメージをインストールして再起動します。

例：

Firepower 1000 および 2100 デバイス

```
firepower 2110 /firmware # show package
Name Package-Vers
-----
cisco-asa-fp2k.9.8.2.SPA 9.8.2
firepower 2110 /firmware # scope auto-install
```

```
firepower 2110 /firmware/auto-install # install security-pack version 9.8.2
The system is currently installed with security software package not set, which has:

- The platform version: not set
If you proceed with the upgrade 9.8.2, it will do the following:
- upgrade to the new platform version 2.2.2.52
- install with CSP asa version 9.8.2
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
  If you proceed the system will be re-imaged. All existing configuration will be
lost,
  and the default configuration applied.
Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

例 :

Cisco Secure Firewall 3100 デバイス

```
firepower 3110 /firmware # show package
Name                                     Package-Vers
-----
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar 7.3.0-14
firepower 3110 /firmware # scope auto-install
firepower 3110 /firmware/auto-install # install security-pack version 9.19.0
The system is currently installed with security software package not set, which has:

- The platform version: not set
If you proceed with the upgrade 9.19.2, it will do the following:
- upgrade to the new platform version 7.0.3-14
- install with CSP asa version 9.19.2
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
  If you proceed the system will be re-imaged. All existing configuration will be
lost,
  and the default configuration applied.
Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.19.0
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

ステップ 7 シャーシのリブートが完了するのを待ちます（5 ～ 10 分）。

FXOS が起動しても、ASA が稼働するまで（5 分）待機する必要があります。次のメッセージが表示されるまで待機します。

Firepower 1000 および 2100 デバイス

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
...
```

Cisco Secure Firewall 3100 デバイス

```
firepower-3110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.19.0.0__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.19.0.0 ...
Verifying signature for cisco-asa.9.19.0.0 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.19.0.0__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
...
```

完全な再イメージ化の実行

この手順では、システム全体を再フォーマットし、イメージを消去して、工場出荷時のデフォルト設定に戻します。この手順を実行する場合は、実行後に新しいソフトウェアイメージをダウンロードして、システムを再設定する必要があります。



(注) この手順を実行すると、管理者パスワードが **Admin123** にリセットされます。

始める前に

- Cisco Secure Firewall 3100 デバイスを Threat Defense バージョン 7.3.0 に再イメージ化するには、ROMMON バージョン 1.1.08 以降が必要です。現在の ROMMON バージョンが 1.1.08 未満の場合は、ASA 9.19 以降にアップグレードして ROMMON をアップグレードする必要があります。Management Center または Device Manager を使用して、Threat Defense のバージョンを 7.3.0 にアップグレードすることもできます（詳細については、Threat Defense を参照してください）。

- この手順を実行するには、コンソールにアクセスする必要があります。
- Threat Defense パッケージを TFTP サーバーまたは USB ドライブに EXT2/3/4 形式か VFAT/FAT32 形式のいずれかでダウンロードします。

参照先 : <https://www.cisco.com/go/ftd-software>

- USBを使用する場合は、開始する前にドライブをインストールします。システムの稼動中に USB デバイスを挿入した場合、USB デバイスを認識させるにはシステムを再起動する必要があります。

手順

ステップ 1 クラウドテナントからデバイスを登録解除します（該当する場合）。クラウドからの登録解除（75 ページ）を参照してください。

ステップ 2 コンソールポートから FXOS CLI に接続します。

管理者アカウントと管理者パスワードを使用してログインします。

ステップ 3 システムを再フォーマットします。

connect local-mgmt

format everything

「yes」と入力すると、デバイスが再起動します。

例 :

```
firepower# connect local-mgmt
firepower(local-mgmt)# format everything
All configuration and bootable images will be lost.
Do you still want to format? (yes/no):yes
```

ステップ 4 ブートアップ中に ROMMON プロンプトを表示するよう要求されたら、Esc を押します。モニタを注視します。

例 :

```
*****
Cisco System ROMMON, Version 1.0.03, RELEASE SOFTWARE
Copyright (c) 1994-2017 by Cisco Systems, Inc.
Compiled Thu 04/06/2017 12:16:16.21 by builder
*****

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM_1/1 : Present
DIMM_2/1 : Present

Platform FPR-2130 with 32768 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 0c:75:bd:08:c9:80
```

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

この時点で、Esc を押します。

ステップ 5 USB ドライブ上の Threat Defense パッケージから EXT2/3/4 または VFAT/FAT32 形式で起動するか、TFTP を使用してネットワークを介して起動します。

USB から起動する場合は、次のようにします。

(注)

システムの稼動中に USB デバイスを挿入した場合、USB デバイスを認識させるにはシステムを再起動する必要があります。

boot usb:/path/filename

ディスクの内容を表示するには、**dir usb:** コマンドを使用します。

例 :

```
rommon 1 > dir usb:
rommon 2 > boot usb:/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-01.sh.REL.tar
```

TFTP から起動する場合は、次のようにします。

管理 1/1 のネットワーク設定を指定し、次の ROMMON コマンドを使用して Threat Defense パッケージをロードします。

address management_ip_address

netmask subnet_mask

server tftp_ip_address

gateway gateway_ip_address

filepath/filename

set

sync

tftpdnld -b

次の情報を参照してください。

- **set** : ネットワーク設定を表示します。 **ping** コマンドを使用してサーバへの接続を確認することもできます。
- **sync** : ネットワーク設定を保存します。
- **tftpdnld -b** : Threat Defense パッケージをロードします。

例 :

```
rommon 1 > address 10.86.118.4
rommon 2 > netmask 255.255.252.0
rommon 3 > server 10.86.118.21
```

```
rommon 4 > gateway 10.86.118.1
rommon 5 > file Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-01.sh.REL.tar
rommon 6 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
  NETMASK=255.255.252.0
  GATEWAY=10.86.118.21
  SERVER=10.86.118.21
  IMAGE=cisco-asa-fp2k.9.8.2.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7 > sync
rommon 8 > tftpdnld -b
Enable boot bundle: tftp_reqsize = 268435456

  ADDRESS: 10.86.118.4
  NETMASK: 255.255.252.0
  GATEWAY: 10.86.118.21
  SERVER: 10.86.118.1
  IMAGE: Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-01.sh.REL.tar
  MACADDR: d4:2c:44:0c:26:00
  VERBOSITY: Progress
  RETRY: 40
  PKTTIMEOUT: 7200
  BLKSIZE: 1460
  CHECKSUM: Yes
  PORT: GbE/1
  PHYMODE: Auto Detect

link up
Receiving Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-01.sh.REL.tar from 10.86.118.21!!!!!!!
[...]
```

サーバーへの接続をトラブルシューティングするには、**Ping** を実行します。

```
rommon 1 > ping 10.86.118.21
Sending 10, 32-byte ICMP Echoes to 10.86.118.21 timeout is 4 seconds
!!!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 2 >
```

(注)

システムが再起動すると、次のエラーが表示されることがあります。

```
firepower-2110 : <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
[F1309][critical][default-infra-version-missing][org-root/fw-infra-pack-default]
Bundle version in firmware package is empty, need to re-install

firepower-3105 FPRM: <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
[F1309][critical][default-infra-version-missing][org-root/fw-infra-pack-default]
Bundle version in firmware package is empty, need to re-install
```

このエラー状態は、この手順で後述するように、新しい Threat Defense ソフトウェアパッケージバージョンをインストールするとすぐに解消されます。

ステップ 6 システムが起動したら、デフォルトのユーザー名 (**admin**) とパスワード (**Admin123**) を使用して FXOS にログインします。

ステップ 7 サーバーから Threat Defense イメージをダウンロードできるように管理インターフェイスを設定します。

USB を使用する場合は、この手順をスキップできます。

- a) ファブリック インターコネクトのスコープを入力します。

scope fabric-interconnect a

- b) 新しい管理 IP 情報を設定します。

set out-of-band static ip ip netmask netmask gw gateway

- c) 設定をコミットします。

commit-buffer

(注)

次のエラーが発生する場合は、変更をコミットする前に DHCP を無効にする必要があります。DHCP を無効にするには、次の手順に従います。

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask> ) is not
in the same network of current DHCP server IP range <ip - ip>.
Either disable DHCP server first or config with a different ipv4 address.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # commit-buffer
```

ステップ 8 Threat Defense パッケージをダウンロードして起動します。USB または TFTP から一時的に起動したので、引き続きローカルディスクにイメージをダウンロードする必要があります。

- a) パッケージをダウンロードします。

scope firmware

download image url

show download-task

パッケージは、以前使用したのと同じ TFTP サーバーまたは USB ドライブ、あるいは管理 1/1 上で到達可能な別のサーバーからダウンロードできます。次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp://username@server/[path/]image_name**
- **scp://username@server/[path/]image_name**
- **sftp://username@server/[path/]image_name**
- **tftp://server[:port]/[path/]image_name**
- **usbA:/path/filename**

例 :

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image
tftp://10.86.118.21/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-01.sh.REL.tar
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
firepower-2110 /firmware # show download-task
Download task:
  File Name Protocol Server      Port      Userid      State
  -----
Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-01.sh.REL.tar
                                Tftp      10.88.29.21      0      Downloaded
```

- b) パッケージのダウンロードが完了（[ダウンロード済み（Downloaded）]の状態）したら、パッケージを起動します。

show package

scope auto-install

install security-pack version version force

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーンが Threat Defense パッケージをインストールして再起動します。

- ステップ9** ソフトウェアパッケージをインストールしたら、ハードウェア プラットフォームのスタートアップガイドにある設定手順を続行します。

管理者パスワードの変更

デバイスを再イメージ化すると、管理者パスワードが Admin123 にリセットされます。初回ログイン時にパスワードを変更するように求められます。パスワードを後で変更する場合、この Threat Defense CLI の手順を使用して管理者パスワードを新しい文字列に変更します。

手順

- ステップ1** Threat Defense アプリケーションの CLI に接続します。

firepower-chassis # **connect ftd**

- ステップ2** **users** テーブルに admin ユーザアカウントがあることを確認します。

> **show user**

例：

```
> show user
Login UID Auth Access Enabled Reset Exp Warn Str Lock Max
admin 100 Local Config Enabled No Never N/A Dis No 0
```

- ステップ3** admin ユーザアカウントの新しいパスワードを設定します。

```
firepower-chassis # configure user password admin
```

例：

```
> configure user password admin
Enter current password:
Enter new password for user admin:
Confirm new password for user admin:
```

Threat Defense がオフラインの場合の管理者パスワードの変更

デバイスを再イメージ化すると、管理者パスワードが Admin123 にリセットされます。初回ログイン時にパスワードを変更するように求められます。パスワードを後で変更する場合、Threat Defense がオフラインなどの理由で使用できないときは、この手順を使用して管理者パスワードを新しい文字列に変更します。Threat Defense がオンラインの場合は、Threat Defense CLI を使用して管理者パスワードを変更する必要があります（[管理者パスワードの変更（73 ページ）](#)を参照）。



（注） FXOS CLI を使用して管理者パスワードを変更する手順は、現在実行している Threat Defense のバージョンによって異なります。

始める前に

- FXOS CLI コンテキストに接続されていることを確認します。シリアルコンソールを介して Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスに接続すると、FXOS CLI コンテキストに自動的に接続されます。Threat Defense CLI コンテキストに接続されている場合は、まず **connect fxos** コマンドを使用して FXOS CLI コンテキストに切り替える必要があります。

手順

ステップ 1 FXOS CLI で、セキュリティのスコープを入力します。

```
firepower # scope security
```

ステップ 2 （Firepower バージョン 6.4 以降）新しいパスワードを設定するには、古い管理者パスワードを再認証する必要があります。

```
firepower /security* # set password
```

例：

```
FPR-2120# scope security
FPR-2120# /security # set password
Enter old password:
Enter new password:
Confirm new password:
firepower-2120 /security* # commit-buffer
```

(Firepower バージョン 6.3 以前) 現在のローカルユーザのリストを表示します。デバイスを再イメージ化したばかりの場合は、このリストに表示されるユーザは **admin** のみになります。

```
firepower /security # show local-user
```

例 :

```
FPR-2120# scope security
FPR-2120 /security # show local-user
User Name      First Name      Last name
-----
admin
```

- a) (Firepower バージョン 6.3 以前) **admin** ローカルユーザのスコープを入力します。

```
firepower /security # enter local-user admin
```

- b) (Firepower バージョン 6.3 以前) ユーザ **admin** の新しいパスワードを設定します。

```
firepower /security/local-user # set password
```

例 :

```
FPR-2100 /security # enter local-user admin
FPR-2100 /security/local-user # set password
Enter a password: cisco
Confirm the password: cisco
```

ステップ 3 設定をコミットします。

```
firepower /security/local-user* # commit-buffer
```

クラウドからの登録解除

Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスを新しい目的（社内の新しいグループに転送する場合、またはサードパーティベンダーからデバイスを購入した場合など）のために、再イメージ化または工場出荷時の状態にリセットする際は、クラウドのテナントからデバイスの登録解除が必要になることがあります。

デバイスが登録されたクラウド（CDO）アカウントにアクセスできる場合は、そのアカウントにログインして Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスを削除します。

クラウドアカウントにアクセスできない場合は、次の手順で FXOS CLI を使用してクラウドテナントから Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスの登録を解除します。

始める前に

- FXOS CLI コンテキストに接続されていることを確認します。シリアルコンソールを介して Firepower 1000/2100 または Cisco Secure Firewall 3100 デバイスに接続すると、FXOS CLI コンテキストに自動的に接続されます。Threat Defense CLI コンテキストに接続されている場合は、まず **connect fxos** コマンドを使用して FXOS CLI コンテキストに切り替える必要があります。
- デバイスがクラウドにアクセスできるかどうかを確認します。

```
firepower # scope fabric a
firepower /fabric-interconnect # show detail
```

show detail の出力に管理 IP アドレスが表示されない場合は、まずデバイスの管理 IP を設定する必要があります

1. ファブリック インターコネクト スコープを開始します。

```
firepower # scope fabric-interconnect
```

2. 新しい管理 IP 情報を設定します。

```
firepower /fabric-interconnect # set out-of-band static ip ip netmask netmask gateway gateway
```

3. 設定をコミットします。

```
firepower /fabric-interconnect # commit buffer
```

手順

-
- ステップ 1** ローカル管理コマンドシェルに接続します。

```
firepower # connect local
```

- ステップ 2** クラウドからデバイスを登録解除します。

```
firepower(local-mgmt)# cloud deregister
```

例

```
firepower # connect local
firepower(local-mgmt) # cloud deregister
```


Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 FXOS トラブルシューティングの履歴

機能名	プラットフォーム	説明
スイッチから mac-filter ドロップパケットをキャプチャ	Cisco Secure Firewall 7.4.1	Cisco Secure Firewall 3100 および 4100 デバイスで、 set drop mac-filter FXOS CLI コマンドを使用して、mac-filter ドロップされたパケットをスイッチからキャプチャできるようになりました。
スイッチパケットパス	Firepower 7.1	portmanager FXOS CLI コマンドを使用して、スイッチパケットパスの問題について Cisco Secure Firewall 3100 デバイスをトラブルシューティングできるようになりました。
クラウドの登録解除	Firepower 6.7	cloud deregister FXOS CLI コマンドを使用して、クラウドテナントから Firepower 1000/2100 デバイスの登録を解除できるようになりました。
管理者パスワードの変更	Firepower 6.4	Firepower バージョン 6.4 以降の Firepower 1000/2100 デバイスでは、新しい管理者パスワードを設定する前に古い管理者パスワードを再認証する必要があります。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。