Cisco Firepower Threat Defense for ISR

Cisco Firepower Threat Defense は、シスコの主要なネットワーク セキュリティ オプションです。ファイアウォール機能、モニタリング、アラート、侵入検知システム（IDS）などの総合的なセキュリティ機能を提供します。

ここでは、Cisco サービス統合型ルータ（ISR）で IDS を設定および導入する方法について説明します。

Cisco Firepower Threat Defense for ISR に関する制限事項

- マルチキャストトラフィックは検査されません。
- IPv6 トラフィックはエクスポートできません。

Cisco Firepower Threat Defense for ISR 関する情報

Cisco FirePOWER Threat Defense for ISR の概要

Cisco Firepower Threat Defense は、パケットフローの検査を強化する優れたセキュリティソリューションです。

Cisco Firepower Threat Defense ソリューションは、次の 2 つのエンティティで構成されています。

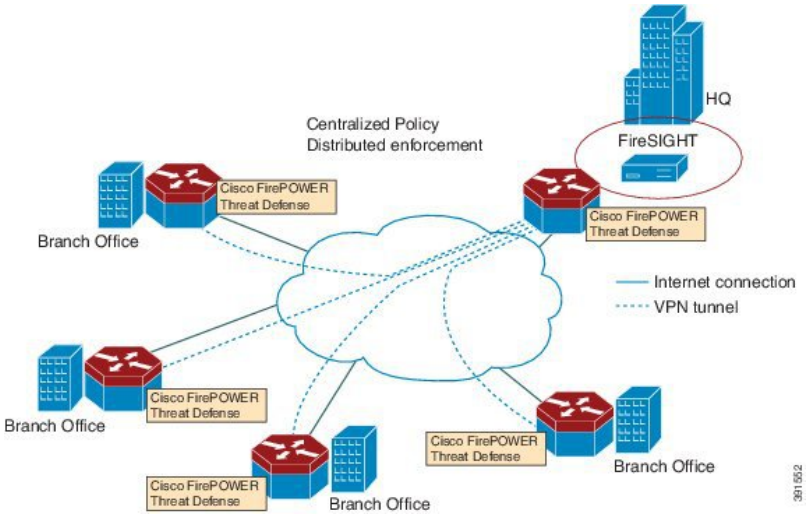
- Cisco FireSIGHT：ネットワーク内の任意の場所で実行できる一元化されたポリシーおよびレポートエンティティ。Cisco FireSIGHT は、Cisco FireSIGHT アプライアンスまたはサーバクラスマシンに仮想インストールしたもののいずれかになります。
- 仮想 Firepower センサー：ポリシーを実装し、イベントと統計情報を防御センターに送り返すセキュリティエンティティ。Firepower センサーは、Cisco 統合型コンピューティングシステム（UCS：Unified Computing System）E シリーズブレードでホストされます。FireSIGHT とセンサーの両方が仮想パッケージとして配布されます。

UCS E シリーズブレードは、第 2 世代（G2）Cisco サービス統合型ルータ（ISR）および Cisco ISR 4000 シリーズサービス統合型ルータ内に収容されている汎用ブレードサーバです。これらのブレードを、オペレーティングシステムのベアメタルとして、またはハイパーバイザの仮想マシンとして導入できます。ルータを UCS E シリーズブレードに接続する内部インターフェイスが 2 つあります。ISR G2 では、Slot0 は周辺機器相互接続エキスプレス（PCIe：Peripheral Component Interconnet Express）の内部インターフェイスであり、UCS E シリーズのスロット 1 はバックプレーン マルチ ギガビット ファブリック（MGF：Multi Gigabit Fabric）に接続されたスイッチドインターフェイスです。Cisco ISR 4000 シリーズルータでは、両方の内部インターフェイスが MGF に接続されます。

ハイパーバイザが UCS E シリーズブレードにインストールされ、Cisco Firepower Threat Defense が仮想マシンとして実行されます。Cisco Firepower Threat Defense の OVA ファイルは、ハイパーバイザ オペレーティング システムを使用して UCS E シリーズブレードに直接インストールされます。Cisco Firepower Threat Defense は、ルータとの追加の通信を行うことなく、匿名のインラインデバイスとして動作します。トラフィックは、入力物理インターフェイスから UCS E シリーズブレードで実行される Cisco Firepower Threat Defense に転送されます。

次の図は、Cisco Firepower Threat Defense の導入の概要を示しています。この図では、センサーと FireSIGHT の間のトラフィックの流れが制御接続となっています。パケットは、ルータの転送ルールを使用し、これらの接続を介してルーティングされます。

図 *1 : Cisco FirePOWER Threat Defense* の導入概要



デフォルトでは、仮想 Cisco Firepower センサーには 3 つのインターフェイスがあり、1 つは管理用、残りの 2 つはトラフィック分析用です。これらのインターフェイスは、UCS E シリーズのインターフェイスにマッピングする必要があります。

UCS ベースのホスティング

Cisco 統合型コンピューティングシステム（UCS）E シリーズブレードは、アプリケーションをホストするための汎用サーバブレードを提供します。このブレードは通常、VMware ESXi ハイパーバイザを実行し、他の VMWare 導入と同様に vSphere を介して管理されます。

Firepower センサーが Cisco UCS E シリーズブレードでホストされている場合は、Cisco Firepower Threat Defense に接続されている Cisco IOS インターフェイスを指定する必要があります。UCS E シリーズブレード内で実行されているアプリケーションは Cisco IOS との互換性が低いため、アプライアンスに接続されているインターフェイスを特定するには、インターフェイスのマッピングを実行する必要があります。Cisco UCS E シリーズブレードに接続するインターフェイスは、ブリッジ ドメイン インターフェイス（BDI）です。

次の Cisco UCS E シリーズブレードは、Firepower センサーのホスティングに対応しています。

- UCS-E 120S
- UCS-E 140D
- UCS-E 140S
- UCS-E 160D
- UCS-E 180D

Cisco Firepower Threat Defense における IDS パケットフロー

Cisco Firepower Threat Defense は、侵入検知システム（IDS）に対応しています。IDS モードでは、トラフィックがセンサーにコピーされ、脅威が分析されます。IDS モードではポリシーを適用できません。違反を検出して報告できます。IDS モードでは、トラフィックはインターフェイスから複製され、Cisco UCS E シリーズブレードで実行される Cisco Firepower Threat Defense にリダイレクトされます。

IDS はトラフィックをコピーし、脅威を検出するためそのトラフィックを分析します。次のいずれかの基準に基づいて、Firepower センサーにパケットを複製する **utd** コマンドを有効にします。

- グローバル検査が有効である場合、ルータを通過するすべてのパケットがセンサーに複製されます。
- インターフェイス単位の検査が有効である場合、入力または出力インターフェイスで検査の **utd** コマンドが有効になっている場合にのみ、パケットが複製されます。

IDS モードでパケット検査を有効にしたインターフェイスを表示するには、**show platform software utd interfaces** コマンドを使用します。パケットの複製は、最初の出力機能の 1 つとして実行されます。

通常のパケット処理では、パケットに適用される機能は、デバイスの設定によって決定される順序付けられたシーケンスを形成します。通常、これらの機能は入力機能または出力機能としてグループ化され、ルーティング機能はこの 2 つの機能の境界を示しています。IDS パケットの複製は、最初の出力機能の1つとして実行されるため、入力機能がパケットをドロップした場合、そのパケットは IDS エンジンへ複製されません。

Firepower センサーのインターフェイス

Firepower センサーの仮想アプライアンスには、トラフィック分析用の 2 つのインターフェイスと FireSIGHT への管理接続用の 1 つのインターフェイスという 3 つのネットワークインターフェイスがあります。2つのトラフィック対応インターフェイスは、設定で2つの仮想インターフェイス「ブリッジ ドメイン インターフェイス（BDI： Bridge Domain Interface）」として表されます。

トラフィックの分析には2つのインターフェイスを使用できますが、侵入検知システム（IDS）には 1 つのトラフィック対応インターフェイスのみ使用できます。

Firepower センサーは管理ネットワークに接続され、LAN セグメント上の別のホストとして表示されます。

（注） 仮想環境で VLAN トラフィックを監視するには、無差別ポートの VLAN ID を 4095 に設定します。

Cisco FirePOWER Threat Defense の相互運用性

Cisco Firepower Threat Defense は、侵入検知システム（IDS）に対応しています。IDS モードでは、選択したトラフィックが分析のために Firepower センサーにコピーされます。

Cisco Firepower Threat Defense は、次の機能と相互運用します。

- ゾーンベースのファイアウォール：アプリケーション レイヤ ゲートウェイ（ALG：Application Layer Gateways）、アプリケーション検査および制御（AIC：Application Inspection and Control）、およびゾーン間で設定されたポリシー
- ネットワークアドレス変換（NAT：Network Address Translation）

（注） Cisco Firepower Threat Defense は、外部グローバルアドレスについて Firepower Threat Defense に通知するメカニズムがないため、外部アドレス変換に対応していません。ただし、外部インターフェイスでアドレス変換を有効にできます。侵入防止システム（IPS）は、常に内部アドレスを使用して、入力インターフェイスの NAT の後、および出力インターフェイスの NAT の前で呼び出されます。

- 暗号
- インテリジェント WAN（IWAN：Intelligent WAN）
- カーネルベースの仮想マシンのワイドエリア アプリケーション サービス（kWAAS：Kernel-based Virtual Machine Wide-Area Application Service）

Cisco Firepower Threat Defense のハードウェアおよびソフトウェア要件

Cisco Firepower Threat Defense ソリューションを実行するには、次のハードウェアが必要です。

- Cisco Firepower センサー（バージョン 5.4）
- Cisco サービス統合型ルータ（ISR）4000 シリーズルータ
- Cisco 統合型コンピューティングシステム（UCS）E シリーズブレード
- Cisco FireSIGHT

Cisco Firepower Threat Defense ソリューションを実行するには、次のソフトウェアが必要です。

- UCS-E ハイパーバイザ
- ESXi 5.0.0、5.1.0、5.5.0
- Cisco Firepower センサー（バージョン Cisco IOS XE リリース 3.14S 以降）
- Cisco FireSIGHT（バージョン 5.2、5.3、5.4）。FireSIGHT は現在のバージョンのみに対応し、直前のバージョンのみとの下位互換性があります。Cisco Firepower センサーのバージョンが 5.4 の場合は、FireSIGHT のバージョン 5.4 または 5.3 を使用する必要があります。

Cisco Firepower Threat Defense ライセンスの取得

Cisco ISR 4000 シリーズサービス統合型ルータには、Cisco Firepower Threat Defense を有効にするためのセキュリティ K9 ライセンスとアプリケーションエクスペリエンス（AppX）ライセンスが必要です。

```
Technology Package License Information:
------------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
appx             appxk9           EvalRightToUse   appxk9
uc               uck9             EvalRightToUse   uck9
security         securityk9       EvalRightToUse   securityk9
ipbase           ipbasek9         Permanent        ipbasek9
```

Cisco Firepower Threat Defense for ISR の導入方法

Cisco Firepower Threat Defense の侵入検知システム（IDS）を導入するには、次のタスクを実行します。

1. Firepower センサーのパッケージを入手します。

2. VMWare VSphere などのハイパーバイザを使用して Firepower センサーのパッケージをインストールします。
3. トラフィックリダイレクションのルータインターフェイスを設定します。
   - Cisco ISR 4000 シリーズルータのブリッジドメインインターフェイス（BDI）の設定。
   - Cisco ISR 第 2 世代ルータの VLAN 設定。
4. Firepower センサーをブートストラップします。
5. Cisco FireSIGHT でポリシーを設定します。
   - ポリシーは FireSIGHT GUI を使用して設定します。
6. 検査を有効にします。

Firepower センサーパッケージの入手

統合型コンピューティングシステム（UCS）E シリーズブレードに Firepower センサーを導入するために、OVA ファイルをダウンロードして保存します。OVA は仮想マシンの圧縮された「インストール可能な」バージョンを含む、オープン仮想アーカイブ（Open Virtualization Archive）です。https://support.sourcefire.com/sections/1/sub_sections/51#5-2-virtual-appliances から OVA ファイルをダウンロードします。

Firepower センサー OVA ファイルのインストール

VMWare VSphere などのハイパーバイザを使用して、UCS E シリーズブレードに Firepower センサー OVA をインストールします。

UCS E シリーズブレードへの Firepower センサーの取り付け

ここでは、Cisco ISR 4000 シリーズサービス統合型ルータにインストールされている統合型コンピューティングシステム（UCS）E シリーズブレードに Firepower センサーを取り付ける方法について説明します。

1. UCS E シリーズカードを取り付けます。
2. **show platform** コマンドを使用して、カードが動作していることを確認します。
3. Cisco 統合型管理コントローラ（CIMC：Cisco Integrated Management Controller）のポートを設定します。

   CIMC GUI は、E シリーズサーバの Web ベースの管理インターフェイスです。CIMC GUI を起動して、次の最小要件を満たしている任意のリモートホストからサーバを管理できます。

   - Java 1.6 以降
   - HTTP または HTTPS に対応
   - Adobe Flash Player 10 以降

   CIMC は、管理（management）という名前のポートで実行されます。次に、管理ポートを IP アドレスでブートストラップする例を示します。

```
ucse subslot 1/0
  imc access-port dedicated
  imc ip-address 10.66.152.158 255.255.255.0
!
```

デフォルトのログインとパスワード（それぞれ admin と password）を使用して、ブラウザから CIMC に接続します。設定例では、ブラウザのアドレスは https://10.66.152.158 です。

4. ESXi をインストールします。

   Cisco UCS E シリーズブレードの ESXi イメージを https://my.vmware.com/web/vmware/details?downloadGroup=CISCO-ESXI-5.1.0-GA-25SEP2012&productId=284 からダウンロードします。

5. VMWare VSphere を使用してCisco UCS E シリーズブレードに Firepower センサーをインストールします。
6. トラフィックリダイレクトを設定します。詳細については、「Cisco UCS E シリーズブレードでのトラフィックリダイレクトの設定」の項を参照してください。
7. VMWare vSwitch を設定します。ISR 4000 シリーズルータの仮想マシン ネットワーク インターフェイス カード（VMNIC：Virtual Machine Network Interface Card）のマッピングは次のとおりです。

   - VMNIC0：ルータバックプレーンの UCS E シリーズのインターフェイス x/0/0 にマッピング
   - VMNIC1：ルータバックプレーンのUCS E シリーズのインターフェイス x/0/1 にマッピング
   - VMNIC2：UCS E シリーズのフロントプレーン GigabitEthernet 2 インターフェイスにマッピング
   - VMNIC3：UCS E シリーズのフロントプレーン GigabitEthernet 3 インターフェイスにマッピング

（注） VMNIC3 は、UCS E シリーズ 140D、160Dm、および 180D でのみ使用できます。

UCS E シリーズ 120S および 140S には、3 つのネットワークアダプタと 1 つの管理ポートがあります。UCS E シリーズ140D、160Dm、および 180D には 4 つのネットワークアダプタがあります。

Cisco UCS E シリーズブレードにおけるトラフィックのリダイレクトの設定

手順の概要

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **no ip address**
5. **no negotiation auto**
6. **switchport mode trunk**
7. **no mop enabled**
8. **no mop sysid**
9. **service instance** *service-instance-number ethernet*
10. **encapsulation dot1q** *vlan-id*
11. **rewrite ingress tag pop** {**1** | **2**} **symmetric**
12. **bridge domain** *bridge-ID*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ucse 1/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no ip address** 例： `Router(config-if)# no ip address`	インターフェイス上で IP アドレスを削除するか、IP 処理を無効にします。
ステップ 5	**no negotiation auto** 例： `Router(config-if)# no negotiation auto`	インターフェイス上で速度、デュプレックスモード、およびフロー制御のアドバタイズメントを無効にします。
ステップ 6	**switchport mode trunk** 例： `Router(config-if)# switchport mode trunk`	トランキング VLAN レイヤ 2 インターフェイスを指定します。
ステップ 7	**no mop enabled** 例： `Router(config-if)# no mop enabled`	インターフェイス上でメンテナンス オペレーション プロトコル（MOP：Maintenance Operation Protocol）を無効にします。
ステップ 8	**no mop sysid** 例：	インターフェイスからの定期的な MOP システム識別メッセージの送信を無効にします。

	コマンドまたはアクション	目的
	`Router(config-if)# no mop sysid`	
ステップ 9	**service instance** *service-instance-number ethernet* 例： `Router(config-if)# service instance 10 ethernet`	インターフェイスでイーサネット サービス インスタンスを設定し、イーサネット サービス インスタンスの設定モードに入ります。
ステップ 10	**encapsulation dot1q** *vlan-id* 例： `Router(config-if-srv)# encapsulation dot1q 10`	インターフェイスの 802.1Q フレーム入力を適切なサービス インスタンスにマップするための一致基準を定義します。
ステップ 11	**rewrite ingress tag pop** {**1** | **2**} **symmetric** 例： `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	サービス インスタンスに入るフレームで実行されるカプセル化調整を指定します。
ステップ 12	**bridge domain** *bridge-ID* 例： `Router(config-if-srv)# bridge domain 10`	サービス インスタンスまたは MAC トンネルをブリッジ ドメイン インスタンスにバインドします。
ステップ 13	**end** 例： `Router(config-if)# end`	イーサネット サービス インスタンスの設定モードを終了し、特権 EXEC 設定モードに戻ります。

Firepower センサーのブートストラップ

Firepower センサーは手動で設定する必要があります。FireSIGHT と通信するように Firepower センサーを設定するには、次のタスクを実行します。詳細については、https://support.sourcefire.com/sections/10 を参照してください。

Cisco 統合型コンピューティングシステム（UCS）E シリーズブレードで実行されているセンサーは、VSphere を介して Firepower センサーの仮想マシンのコンソールにログインすることによってブートストラップされます。

（注） Firepowerセンサーは、ブートストラップする前にインストールして導入する必要があります。

手順の概要

1. ログインするためのデフォルトのユーザ名とパスワードを入力します。
2. **configure network ipv4 manual** *ip-address network-mask default-gateway*
3. **configure network dns servers** *dns-server*
4. **configure network dns searchdomains** *domain-name*
5. **configure manager add** *dc-hostname registration-key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ログインするためのデフォルトのユーザ名とパスワードを入力します。	センサーを設定する場合、デフォルトのユーザ名とパスワードはそれぞれ admin と Sourcefire となります。 • Firepowerセンサーに初めてログインした後は、管理者パスワードを変更する必要があります。
ステップ 2	**configure network ipv4 manual** *ip-address network-mask default-gateway* 例： `Device# configure network ipv4 manual 10.66.152.137 255.255.255.0 10.66.152.1`	ネットワーク接続を設定します。
ステップ 3	**configure network dns servers** *dns-server* 例： `Device# configure network dns servers 192.10.26.10`	ドメインネームシステム（DNS：Domain Name System）サーバを設定します。
ステップ 4	**configure network dns searchdomains** *domain-name* 例： `Device# configure network dns searchdomains cisco.com`	DNS 検索ドメインを設定します。
ステップ 5	**configure manager add** *dc-hostname registration-key* 例： `Device# configure manager sourcefire-dc.cisco.com cisco-sf`	センサーを FireSIGHT に関連付けます。 • *registration key*は、ユーザが FireSIGHT にセンサーを登録するために後で使用する文字列です。

例

次は、Firepower センサーの設定済みのネットワーク設定を表示する **show network** コマンドからの出力例です。

```
Device# show network

-------------------------------------------------
IPv4
Configuration             : manual
Address                   : 10.66.152.137
Netmask                   : 255.255.255.0
Gateway                   : 10.66.152.1
MAC Address               : 44:03:A7:43:05:AD
Management port           : 8305
-------------------------------------------------
IPv6
Configuration             : disabled
Management port           : 8305
```

```
-----------------------------------------------------
```

次は、設定済みの DNS 設定を表示する **show dns** コマンドからの出力例です。

```
Device# show dns

search cisco.com
nameserver 192.10.26.10
```

次は、設定済みの管理設定を表示する **show managers** コマンドからの出力例です。

```
Device# show managers

Host                        : sourcefire-dc.cisco.com
Registration Key            : cisco-sf
Registration                : pending
RPC Status                  :
```

IDS 検査のグローバルな有効化

要件に基づいて、グローバルレベルまたはインターフェイスレベルで侵入検知システム（IDS）の検査を設定できます。

専用の管理インターフェイスでは IDS 検査を有効にできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **utd enable**
4. **utd engine advanced**
5. **threat detection**
6. **exit**
7. **utd**
8. **all-interfaces**
9. **engine advanced**
10. **fail close**
11. **rate** *pps-rate*
12. **redirect-interface** *interface interface-number*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**utd enable** 例： `Router(config)# utd enable`	統合脅威防御の設定モードに入ります。
ステップ 4	**utd engine advanced** 例： `Router(config)# utd engine advanced`	統合脅威防御（UTD）の拡張エンジンを設定し、UTD の拡張エンジンの設定に入ります。 モードで使用します。
ステップ 5	**threat detection** 例： `Router(config-utd-eng-adv)# threat detection`	脅威検知または侵入防止システム（IPS）を Snort エンジンの動作モードとして設定します。
ステップ 6	**exit** 例： `Router(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 7	**utd** 例： `Router(config)# utd`	統合脅威防御の設定モードに入ります。
ステップ 8	**all-interfaces** 例： `Router(config-utd)# all-interfaces`	デバイスのすべてのレイヤ3インターフェイスで UTD を設定します。
ステップ 9	**engine advanced** 例： `outer(config-utd)# engine advanced`	統合脅威防御（UTD）の拡張エンジンを設定し、UTD の拡張エンジンの設定に入ります。
ステップ 10	**fail close** 例： `Device(config-engine-std)# fail close`	（オプション）UTD エンジンに障害が発生した場合に行うアクションを定義します。デフォルトのオプションはフェールオープンです。フェールクローズオプションは、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックをドロップします。フェールオープンオプションを使用すると、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックを許可します。

	コマンドまたはアクション	目的
ステップ 11	**rate** *pps-rate* 例： `Device(config-engine-std)# rate 2000000`	（オプション）センサーにプッシュする pps レートを指定します。指定できる範囲は 1000 ～ 4000000 です。
ステップ 12	**redirect-interface** *interface interface-number* 例： `Router(config-utd)# redirect-interface BDI 10`	インターフェイスで IDS のトラフィックリダイレクトを設定します。
ステップ 13	**end** 例： `Router(config-utd)# end`	統合脅威防御の設定モードを終了し、特権 EXEC モードに戻ります。

インターフェイスごとの IDS 検査の有効化

要件に基づいて、グローバルレベルまたはインターフェイスレベルで侵入検知システム（IDS）の検査を設定できます。

専用の管理インターフェイスでは IDS 検査を有効にできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **utd enable**
5. **exit**
6. IDS 検査を必要とするすべてのインターフェイスで、手順 3 ー 5 を繰り返します。管理インターフェイスで検査を設定しないでください。
7. **utd engine advanced**
8. **threat detection**
9. **utd**
10. **engine advanced**
11. **fail close**
12. **rate** *range*
13. **redirect interface** *type number*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**utd enable** 例： `Router(config-if)# utd enable`	インターフェイスで侵入検知を有効にします。
ステップ 5	**exit** 例： `Router(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 6	IDS 検査を必要とするすべてのインターフェイスで、手順3ー5を繰り返します。管理インターフェイスで検査を設定しないでください。	-
ステップ 7	**utd engine advanced** 例： `Router(config)# utd engine advanced`	統合脅威防御（UTD）の拡張エンジンを設定し、UTD の拡張エンジンの設定に入ります。 モードで使用します。
ステップ 8	**threat detection** 例： `Router(config-utd-eng-adv)# threat detection`	脅威検知または侵入防止システム（IPS）を Snort エンジンの動作モードとして設定します。
ステップ 9	**utd** 例： `Router(config)# utd`	統合脅威防御の設定モードに入ります。
ステップ 10	**engine advanced** 例： `outer(config-utd)# engine advanced`	統合脅威防御（UTD）の拡張エンジンを設定し、UTD の拡張エンジンの設定に入ります。
ステップ 11	**fail close** 例： `Device(config-engine-std)# fail close`	（オプション）UTD エンジンに障害が発生した場合に行うアクションを定義します。デフォルトのオプションはフェールオープンです。フェールクローズオプションは、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックをドロップします。フェールオープンオプションを使用すると、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックを許可します。

	コマンドまたはアクション	目的
ステップ 12	**rate** *range* 例： `Device(config-engine-std)# rate 1000`	（オプション）センサーにプッシュする pps レートを指定します。指定できる範囲は 1000 ～ 4000000 です。
ステップ 13	**redirect interface** *type number* 例： `Router(config-utd)# redirect interface BDI 10`	インターフェイスで IDS のトラフィックリダイレクトを設定します。
ステップ 14	**end** 例： `Router(config-utd)# end`	統合脅威防御の設定モードを終了し、特権 EXEC モードに戻ります。

ISR での Cisco Firepower Threat Defense の設定例

例：Cisco UCS E シリーズブレードでのトラフィックリダイレクトの設定

次に、トラフィックリダイレクトの入力および出力インターフェイスを設定する例を示します。

```
Router# configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# no ip address
Router(config-if)# no negotiation auto
Router(config-if)# switchport mode trunk
Router(config-if)# no mop enabled
Router(config-if)# no mop sysid
Router(config-if)# exit
Router(config)# interface ucse 1/0/1
Router(config-if)# no ip address
Router(config-if)# no negotiation auto
Router(config-if)# switchport mode trunk
Router(config-if)# no mop enabled
Router(config-if)# no mop sysid
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge domain 10
Router(config-if-srv)# exit
Router(config-if)# exit
Router(config)# interface BDI 10
Router(config-if)# no shutdown
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if-srv)# end
```

例：Firepower センサーのブートストラップ

次に、Firepower Threat Defense センサーをブートストラップする例を示します。

```
Sourcefire3D login: admin
Password: Sourcefire
Last login: Tue Nov 12 11:15:03 UTC 2013 on tty1

Copyright 2001-2013, Sourcefire, Inc. All rights reserved. Sourcefire is
a registered trademark of Sourcefire, Inc. All other trademarks are
property of their respective owners.

Sourcefire Linux OS v5.2.0 (build 135)
Sourcefire Virtual Device 64bit v5.2.0 (build 838)

> configure password
Enter current password:
Enter new password:
Confirm new password:

> configure network ipv4 manual 10.66.152.137 255.255.255.0 10.66.152.1
Setting IPv4 network configuration.
ADDRCONF(NETDEV_UP): eth0: link is not ready
e1000: eth0: e1000_phy_read_status: Error reading PHY register
e1000: eth0: e1000_watchdog_task: NIC Link is Up
1000 Mbps Full Duplex, Flow Control: None
ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready

Network settings changed.

> configure network dns servers 192.10.26.10

> configure network dns searchdomains cisco.com

configure manager add sourcefire-dc.cisco.com cisco-sf
Manager successfully configured.
```

例：IDS 検査のグローバルな有効化

```
Router# configure terminal
Router(config)# utd enable
Router(config-utd)# utd engine advanced
Router(config-utd-adv)# threat detection
Router(config-utd-adv)# exit
Router(config)# utd
Router(config-utd)# all-interfaces
Router(config-utd)# engine advanced
Router(config-utd)# fail close
Router(config-utd)# rate 1000
Router(config-utd)# redirect-interface BDI 10
Router(config-utd)# end
```

例：インターフェイスごとの IDS 検査の有効化

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# utd enable
Router(config-utd)# utd engine advanced
Router(config-utd-adv)# threat detection
Router(config-utd-adv)# exit
Router(config)# utd
Router(config-utd)# engine advanced
Router(config-utd)# fail close
Router(config-utd)# rate 1000
Router(config-utd)# redirect-interface BDI 10
Router(config-utd)# end
```

IDS 検査の確認とモニタリング

次のコマンドを使用して、侵入検知システム（IDS）の導入を確認およびモニタします。

手順の概要

1. **enable**
2. **debug platform condition feature utd controlplane**
3. **debug platform condition feature utd dataplane submode**
4. **show platform hardware qfp active utd** {**config** | **status** [**all**] [**clear**] [**drop**] [**general**]}

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 debug platform condition feature utd controlplane

IDS 設定およびステータス情報のデバッグを有効にします。

例：

```
Router# debug platform condition feature utd controlplane

network RF:
  network-rf idb-sync-history events debugging is on
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

Feature      Type           Submode       Level
```

```
------------|-------------|------------------------------
UTD           controlplane                info

IOSXE Packet Tracing Configs:

Packet Infra debugs:

Ip Address                                                 Port
-----------------------------------------------------------|----------
```

ステップ 3 debug platform condition feature utd dataplane submode

IDS パケットフロー情報のデバッグを有効にします。

例：

```
Router# debug platform  condition feature utd dataplane submode

network RF:
  network-rf idb-sync-history events debugging is on
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

Feature      Type            Submode                    Level
-----------|-------------|---------------------|----------
UTD           controlplane                            info
UTD           dataplane     fia proxy punt            info

IOSXE Packet Tracing Configs:

Packet Infra debugs:

Ip Address                                                 Port
-----------------------------------------------------------|----------
```

ステップ 4 show platform hardware qfp active utd {config | status [all] [clear] [drop] [general]}

Cisco クォンタムフロープロセッサ（QFP：Quantum Flow Processor）の IDS 検査に関する情報を表示します。

例：

```
Router# show platform hardware qfp active utd config

Global flags: 0x40004
Num divert interfaces: 1
Divert UIDBs: 65521 0
FIB information
[0][0] 0x309e3c30
[0][1] 0x0
[1][0] 0x309e4040
[1][1] 0x0
```

Cisco Firepower Threat Defense for ISR に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
IOS コマンド	『Cisco IOS Master Command List, All Releases』[英語]
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
UCS E シリーズ サーバ	http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/2-0/gs/guide/b_2_0_Ge

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Cisco FirePOWER Threat Defense for ISR の機能に関する情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : Cisco FirePOWER Threat Defense for ISR* の機能に関する情報

機能名	リリース	機能情報

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。