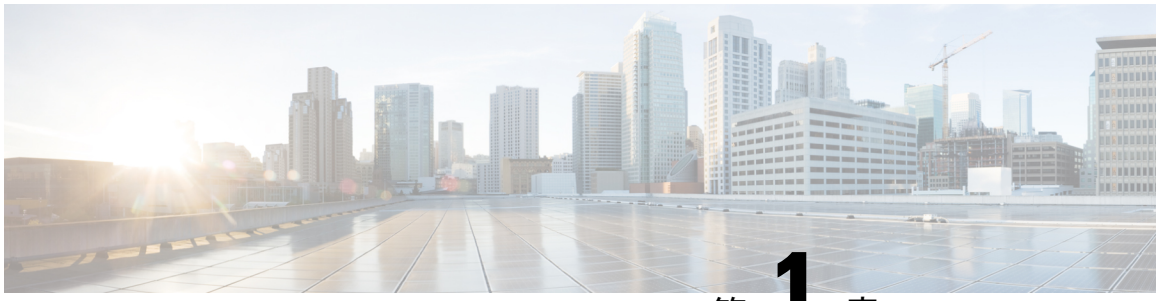
# Cisco IOS XE 17 統合脅威防御セキュリティ コンフィギュレーション ガイド


**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/

# 目 次



第 1 章

# 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。



## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

## 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。

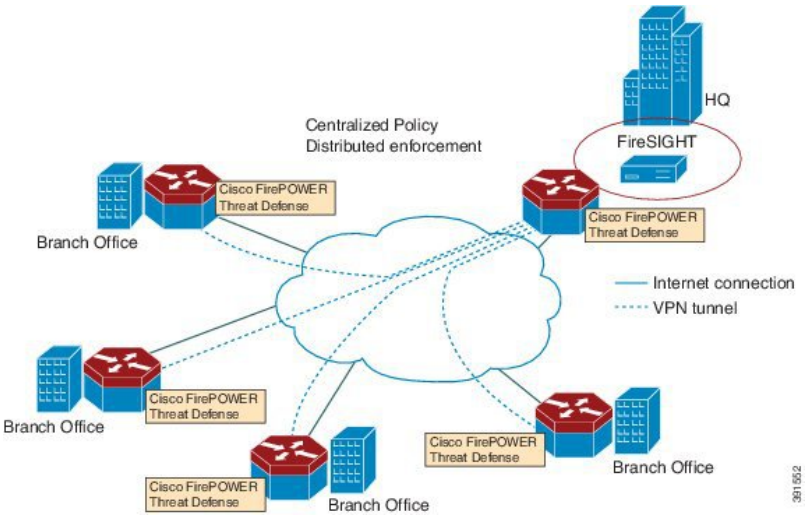
- Cisco FireSIGHT：ネットワーク内の任意の場所で実行できる一元化されたポリシーおよびレポートエンティティ。Cisco FireSIGHT は、Cisco FireSIGHT アプライアンスまたはサーバクラスマシンに仮想インストールしたもののいずれかになります。
- 仮想 Firepower センサー：ポリシーを実装し、イベントと統計情報を防御センターに送り返すセキュリティエンティティ。Firepower センサーは、Cisco 統合型コンピューティングシステム（UCS：Unified Computing System）E シリーズブレードでホストされます。FireSIGHT と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**<br>例：<br>`Router> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Router# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **interface** *type number*<br>例：<br>`Router(config)# interface ucse 1/0/0` | インターフェイスを設定し、インターフェイス設定モードを開始します。 |
| ステップ 4 | **no ip address**<br>例：<br>`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**<br>例：<br>`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**<br>例：<br>`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**<br>例：<br>`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**<br>例：<br>`Router(config-if)# no mop sysid` | 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。 |
| ステップ 9 | **service instance** *service-instance-number ethernet*<br>例：<br>`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*<br>例：<br>`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**<br>例：<br>`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*<br>例： | 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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Router(config-if-srv)# bridge domain 10` | |
| ステップ 13 | **end**<br>例：<br>`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。<br>• 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*<br>例：<br>`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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **configure network dns servers** *dns-server*<br>例：<br>`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*<br>例：<br>`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*<br>例：<br>`Device# configure manager sourcefire-dc.cisco.com cisco-sf` | センサーを FireSIGHT に関連付けます。<br>• *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**<br>例：<br>`Router> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Router# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **utd enable**<br>例：<br>`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**<br>例：<br>`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。<br>モードで使用します。 |
| ステップ 5 | **threat detection**<br>例：<br>`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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **exit**<br>例：<br>`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**<br>例：<br>`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**<br>例：<br>`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**<br>例：<br>`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**<br>例：<br>`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。 |
| ステップ 11 | **rate** *pps-rate*<br>例：<br>`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*<br>例：<br>`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**<br>例：<br>`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**<br>例：<br>`Router> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Router# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **interface** *type number*<br>例：<br>`Router(config)# interface gigabitethernet 0/1/1` | インターフェイスを設定し、インターフェイス設定モードを開始します。 |
| ステップ 4 | **utd enable**<br>例：<br>`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**<br>例：<br>`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。 | - |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 7 | **utd engine advanced**<br>例：<br>`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。<br>モードで使用します。 |
| ステップ 8 | **threat detection**<br>例：<br>`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**<br>例：<br>`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**<br>例：<br>`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**<br>例：<br>`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。 |
| ステップ 12 | **rate** *range*<br>例：<br>`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*<br>例：<br>`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**<br>例：<br>`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]<br>• 『Cisco IOS Security Command Reference: Commands D to L』[英語]<br>• 『Cisco IOS Security Command Reference: Commands M to R』[英語]<br>• 『Cisco IOS Security Command Reference: Commands S to Z』[英語] |

| 関連項目 | マニュアル タイトル |
|---|---|
| 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_Gettin |

### 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。<br>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。<br>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 |

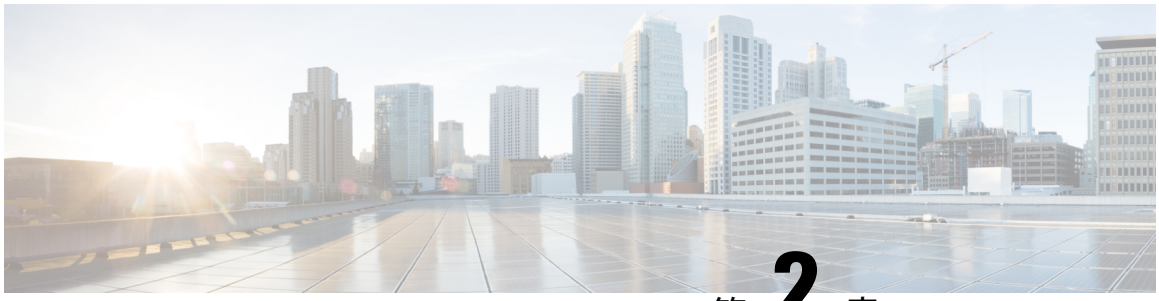
# Cisco FirePOWER Threat Defense for ISR の機能に関する情報

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 |
|---|---|---|
| Cisco Firepower Threat Defense for ISR | Cisco IOS XE リリース 3.14S | Cisco Firepower Threat Defense は、優れた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）などの幅広いセキュリティ機能を搭載しています。<br>この機能は、Cisco ISR 4000 シリーズサービス統合ルータに導入されています。<br>次のコマンドが導入または変更されました：**debug platform condition feature utd controlplane**、**debug platform condition feature utd dataplane submode**、**ids**、**mode (utd)**、**show platform hardware qfp active feature utd**、**service utd**、**utd**、**utd ids** |
| Cisco Firepower Threat Defense for ISR | Cisco IOS リリース 15.5（1）T | Cisco Firepower Threat Defense は、優れた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）などの幅広いセキュリティ機能を搭載しています。<br>次のコマンドが導入または変更されました。**ids**、**utd** |



第 2 章

# Snort IPS

Snort IPS 機能は、Cisco 4000 シリーズサービス統合型ルータおよび Cisco クラウドサービスルータ 1000v シリーズのブランチオフィスで侵入防止システム（IPS）または侵入検知システム（IDS）を実現します。この機能は、オープンソースの Snort ソリューションを使用して IPS と IDS を有効にします。Snort IPS 機能は、Cisco IOS XE リリース 3.16.1S、3.17S、およびそれ以降のリリースで使用できます。

（注） 仮想ルーティングおよび転送（VRF）機能は、Cisco IOS XE Denali リリース16.3.1 以降のリリースの Snort IPS 設定に対応しています。

ここでは、その機能および動作の仕組みについて説明します。



## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してくださ

い。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

# Snort IPS の制約事項

Snort IPS 機能には、次のような制約事項が適用されます。

- Cisco 4000 シリーズ ISR でブーストライセンスを有効にした場合、Snort IPS の仮想サービスコンテナを設定できません。
- ゾーンベース型ファイアウォールの SYN クッキー機能と互換性がありません。
- ネットワークアドレス変換 64（NAT64）には対応しません。
- オープンソースの Snort での SNMP ポーリングには、SnortSnmp プラグインが必要となります。SnortSnmp プラグインが UTD にインストールされていないため、Snort IPS は SNMP ポーリング機能または MIB に対応しません。
- **IOS syslog はレートが制限されているため、Snort によって生成されたすべてのアラートが IOS Syslog で表示されない場合があります。ただし、外部ログサーバにエクスポートする場合は、すべての Syslog メッセージを表示できます。**

# Snort IPS に関する情報

## Snort IPS の概要

Snort IPS 機能は、Cisco 4000 シリーズサービス統合型ルータおよび Cisco クラウドサービスルータ 1000v シリーズのブランチオフィスで侵入防止システム（IPS）または侵入検知システム（IDS）を実現します。この機能は、Snort エンジンを使用して IPS および IDS 機能を実現します。

Snort は、リアルタイムでトラフィック分析を行い、IP ネットワークで脅威が検出されたときにアラートを生成するオープンソースのネットワーク IPS です。また、プロトコル分析、コンテンツ検索またはマッチングを実行し、バッファオーバーフロー、ステルスポートスキャンなどのさまざまな攻撃やプローブを検出することもできます。Snort エンジンは、Cisco 4000 シリーズサービス統合型ルータおよび Cisco クラウドサービスルータ 1000v シリーズで仮想コンテナサービスとして実行されます。

Snort IPS 機能は、IPS または IDS 機能を提供するネットワーク侵入検知および防止モードで動作します。ネットワーク侵入検知および防止モードでは、Snort は次のアクションを実行します。

- ネットワークトラフィックをモニタし、定義されたルールセットに照らしあわせて分析します。
- 攻撃の分類を行います。
- 一致したルールに照らしあわせてアクションを呼び出します。

要件に応じて、IPS または IDS モードで Snort を有効にできます。IDS モードでは、Snort はトラフィックを検査し、アラートを報告しますが、攻撃を防ぐためのアクションは実行しません。IPS モードでは、侵入検知に加えて、攻撃を防ぐためのアクションを実行します。

Snort IPS はトラフィックをモニタし、イベントを外部ログサーバまたは IOS syslog に報告します。IOS syslog へのロギングを有効にすると、ログメッセージが大量に発生する可能性があるため、パフォーマンスに影響する場合があります。Snort ログに対応する外部のサードパーティ製のモニタリングツールを、ログの収集と分析に使用できます。

# Snort IPS 署名パッケージ

UTD OVA は、ルータのセキュリティライセンスに含まれています。デフォルトでは、ルータにはコミュニティ署名パッケージのみがロードされています。サブスクリプションには次の 2 つのタイプがあります。

- コミュニティ署名パッケージ
- サブスクライバベースの署名パッケージ

コミュニティ署名パッケージのルールセットは、脅威に対する限定的な防御を提供します。サブスクライバベースの署名パッケージのルールセットは、脅威に対する最良の防御を提供します。これには、エクスプロイトの前のカバレッジが含まれているため、セキュリティインシデントまたは新しい脅威のプロアクティブな検出に応じて、更新された署名に最速でアクセスできます。このサブスクリプションはシスコによって完全にサポートされており、パッケージは Cisco.com でアップデートされます。サブスクライバベースの署名パッケージは、ソフトウェアのダウンロードページからダウンロードできます。

ユーザがソフトウェアのダウンロードページから署名パッケージを手動でダウンロードする場合、パッケージのバージョンが Snort エンジンのバージョンと同じであることを確認する必要があります。たとえば、Snort エンジンのバージョンが 2982 の場合、ユーザは同じバージョンの署名パッケージをダウンロードする必要があります。バージョンが一致しないと、署名パッケージのアップデートは拒否され、失敗します。

（注） 署名パッケージがアップデートされると、データプレーンのフェールオープンまたはフェールクローズ設定に応じて、エンジンが再起動され、トラフィックが短時間中断されるか、もしくは検知がバイパスされます。

# 署名更新でサポートされるCisco IOS XEのリリースおよびUTDパッケージの最小バージョン

次の表 1 に、Cisco IOS XE の最小リリースと、2020 年 1 月以降の署名パッケージのアップデートに対応する各 UTD パッケージのバージョンを示します。表に示されているものより前の Cisco IOS XE のリリースおよび各 UTD パッケージのバージョンには対応していません。表に記載されているものよりも新しい Cisco IOS XE のリリースおよび各 UTD パッケージのバージョンには、最初のリリースから対応しています。

**表 *2: UTD* 署名パッケージのアップデート対応バージョンのマトリックス**

| Cisco IOS XE リリース | UTD パッケージのバージョン |
|---|---|
| 16.6.7 | 1.0.10_SV29111_XE_16_6 |
| 16.9.4 | 1.0.4_SV29111_XE_16_9 |
| 16.10.2 | 1.0.9_SV2.9.11.1_XE16.10 |

（注） UTD がオーバーサブスクライブされると、脅威防御チャネルの状態が緑と赤の間で変化します。UTD データプレーンは、フェールクローズが設定されている場合はそれ以降のすべてのパケットをドロップするか、フェールクローズが設定されていない場合は検査されてないパケットを転送します（デフォルト）。UTD サービスプレーンがオーバーサブスクリプションから回復すると、緑色のステータスで UTD データプレーンに応答します。

# Snort IPS ソリューション

Snort IPS ソリューションは、次のエンティティで構成されています。

- Snort センサー：トラフィックをモニタして、設定されたセキュリティポリシー（署名、統計情報、プロトコル分析など）に基づいて異常を検出し、アラートサーバまたはレポートサーバにアラートメッセージを送信します。Snort センサーは、仮想コンテナサービスとしてルータに導入されます。
- 署名ストア：定期的に更新される Cisco 署名パッケージをホストします。これらの署名パッケージは、定期的にもしくはオンデマンドで Snort センサーにダウンロードされます。検証済みの署名パッケージは Cisco.com に掲載されます。設定に基づいて、署名パッケージを Cisco.com またはローカルサーバからダウンロードできます。

（注） 署名パッケージを保持するためにローカルサーバから署名パッケージをダウンロードする場合は、HTTP のみに対応します。

Snort センサーが署名パッケージを取得するには、Cisco.com の認証情報を使用して、署名パッケージを Cisco.com からローカルサーバに手動でダウンロードする必要があります。

URL が IP アドレスとして指定されていない場合、Snort コンテナは（ルータに設定された DNS サーバ上で）ドメイン名ルックアップを実行して、Cisco.com によるまたはローカルサーバ上の自動署名更新の場所を解決します 。

- アラートまたはレポートサーバ：Snort センサーからアラートイベントを受信します。Snort センサーによって生成されたアラートイベントは、IOS syslog または外部 syslog サーバ、もしくは IOS syslog と外部 syslog サーバの両方に送信できます。Snort IPS ソリューションに付属している外部ログサーバはありません。
- 管理：Snort IPS ソリューションを管理します。管理は、IOS CLI を使用して設定します。Snort センサーには直接アクセスできず、すべての設定は IOS CLI を使用してのみ行えます。

# Snort 仮想サービスインターフェイスの概要

Snort センサーは、ルータ上でサービスとして動作します。サービスコンテナは、仮想テクノロジーを使用して、アプリケーション用の Cisco デバイスにホスティング環境を提供します。

Snort トラフィック検査は、インターフェイス単位で、または対応しているすべてのインターフェイスでグローバルに有効にできます。検査対象のトラフィックは Snort センサーに転送され、再度投入されます。侵入検知システム（IDS）では、識別された脅威がログイベントとして報告され、許可されます。ただし、侵入防止システム（IPS）では、ログイベントとともに攻撃を防ぐためのアクションが実行されます。

Snort センサーには 2 つの VirtualPortGroup インターフェイスが必要です。最初の VirtualPortGroup インターフェイスは管理トラフィックに使用され、2 つ目は転送プレーンと Snort 仮想コンテナサービス間のデータトラフィックに使用されます。これらの VirtualPortGroup インターフェイスには、ゲスト IP アドレスを設定する必要があります。管理 VirtualPortGroup インターフェイスに割り当てられた IP サブネットは、署名サーバおよびアラート / 報告サーバと通信できる必要があります。

2 つ目の VirtualPortGroup インターフェイスの IP サブネットは、このインターフェイス上のトラフィックがルータ内部にあるため、カスタマーネットワーク上でルーティング可能であってはなりません。内部サブネットを外部に公開することはセキュリティ上のリスクとなります。2 つ目の VirtualPortGroup サブネットには 192.0.2.0/30 の IP アドレス範囲を使用することをお勧めします。192.0.2.0/24 のサブネットを使用することは、RFC 3330 で定義されています。

管理トラフィック用の **virtual-service** コマンドを使って管理インターフェイスを使用することもできます。管理インターフェイスを設定する場合、2 つの VirtualPortGroup インターフェイスが必要となります。ただし、最初の VirtualPortGroup インターフェイスには **guest ip address** を設定しないでください。

仮想サービスが実行されているルータと同じ管理ネットワークで、Snort 仮想コンテナサービスの IP アドレスを割り当てることができます。この設定は、syslog またはアップデートサーバが管理ネットワーク上にあり、他のインターフェイスからアクセスできない場合に役立ちます。

# 仮想サービスのリソースプロファイル

Snort IPS 仮想サービスは、低、中、高という 3 つのリソースプロファイルに対応しています。これらのプロファイルは、仮想サービスの実行に必要な CPU およびメモリリソースを表示します。これらのリソースプロファイルの 1 つを設定できます。リソースプロファイルの設定は任意です。プロファイルを設定しない場合、仮想サービスはデフォルトのリソースプロファイルでアクティブ化されます。次の表に、Cisco 4000 シリーズ ISR および Cisco クラウドサービスルータ 1000v シリーズのリソースプロファイルの詳細を示します。

| プラットフォーム | プロファイル | 仮想サービスのリソース要件 | | プラットフォーム要件 |
|---|---|---|---|---|
| | | システム CPU | メモリ | |
| Cisco 4321 ISR | デフォルト | 50% | 最小：1 GB（RAM）<br>最小：750 MB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| Cisco 4331 ISR | 低（デフォルト） | 25% | 最小：1 GB（RAM）<br>最小：750 MB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| | 中 | 50% | 最小：2 GB（RAM）<br>最小：1 GB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| | 高 | 75% | 最小：4 GB（RAM）<br>最小：2 GB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |

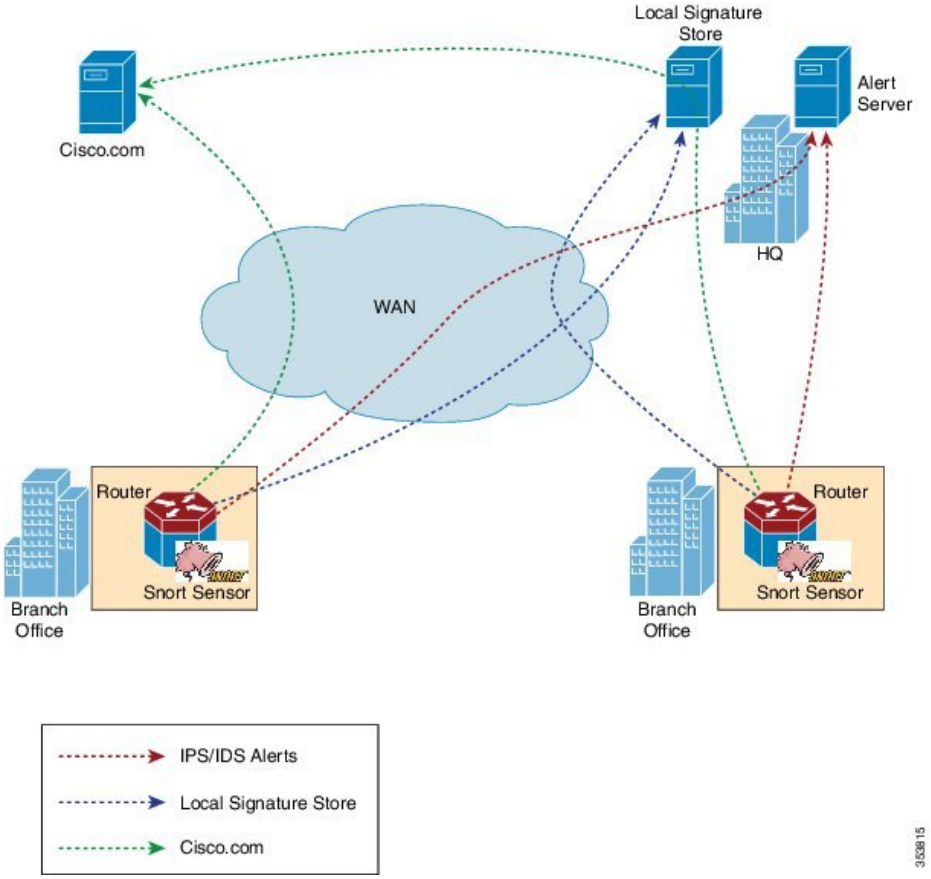
| プラットフォーム | プロファイル | 仮想サービスのリソース要件 | | プラットフォーム要件 |
|---|---|---|---|---|
| | | システム CPU | メモリ | |
| Cisco 4351 ISR | 低（デフォルト） | 25% | 最小：1 GB（RAM）<br>最小：750 MB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| | 中 | 50% | 最小：2 GB（RAM）<br>最小：1 GB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| | 高 | 75% | 最小：4 GB（RAM）<br>最小：2 GB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| Cisco 4431 ISR | 低（デフォルト） | 25% | 最小：1 GB（RAM）<br>最小：750 MB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| | 中 | 50% | 最小：2 GB（RAM）<br>最小：1 GB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| | 高 | 75% | 最小：4 GB（RAM）<br>最小：2 GB（ディスクまたはフラッシュ） | 最小：12 GB（RAM）<br>最小：12 GB（ディスクまたはフラッシュ） |

| プラットフォーム | プロファイル | 仮想サービスのリソース要件 | | プラットフォーム要件 |
|---|---|---|---|---|
| | | システム CPU | メモリ | |
| Cisco 4451 ISR | 低（デフォルト） | 25% | 最小：1 GB（RAM）<br>最小：750 MB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| | 中 | 50% | 最小：2 GB（RAM）<br>最小：1 GB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| | 高 | 75% | 最小：4 GB（RAM）<br>最小：2 GB（ディスクまたはフラッシュ） | 最小：12 GB（RAM）<br>最小：12 GB（ディスクまたはフラッシュ） |
| Cisco CSR 1000V | 低（デフォルト） | 25% | 最小：1 GB（RAM）<br>最小：750 MB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| | 中 | 50% | 最小：2 GB（RAM）<br>最小：1 GB（ディスクまたはフラッシュ） | 最小：8 GB（RAM）<br>最小：8 GB（ディスクまたはフラッシュ） |
| | 高 | 75% | 最小：3 GB（RAM）<br>最小：2 GB（ディスクまたはフラッシュ） | 最小：12 GB（RAM）<br>最小：12 GB（ディスクまたはフラッシュ） |

# Snort IPS の導入

次の図は、Snort IPS の導入概要を示しています。

図 *2 : Snort IPS* の展開概要




次の手順では、Snort IPS ソリューションの導入について説明します。

- Snort OVA ファイルを Cisco ルータにコピー、インストール、アクティブ化する。
- 署名パッケージを、Cisco.com または設定済みのローカルサーバから Cisco ルータにダウンロードする。
- ネットワーク侵入検知またはネットワーク防御機能を設定する。
- アラートおよびレポートサーバを、Snort センサーからアラートを受信するように設定する。

# 脅威検知アラートの可視性

Cisco IOS XE Fuji 16.8 リリースから、次の脅威検知アラートの要約詳細情報を取得できます。

- 上位 10 の脅威検知アラート（IDS または IPS）およびカウントが直近の 24 時間に要約されます。
- 直近の 24 時間の各署名 ID の上位 10 件の SIP、DIP、および VRF のサマリー。

（注） 直近の 24 時間とは、CLI を使用してアラートの概要を要求した時点から 24 時間前までの期間を表します。

可視化機能は、シングルテナントでのみ使用でき、マルチテナントでは使用できません。

アラートの概要を表示するには、**show utd engine standard logging threat-inspection statistics** *detail* コマンドを使用します。

### 脅威検知アラートのロギングの有効化と無効化

脅威検知アラートの統計情報のロギングを有効にするには、次の手順を実行します。

```
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#logging statistics enable
Router(config-utd-engstd-insp)#exit
```

脅威検知アラートの統計情報のロギングを無効にするには、次の手順を実行します。

```
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#no logging statistics enable
Router(config-utd-engstd-insp)#exit
```

# Snort IPS の導入方法

対応しているデバイスに Snort IPS を導入するには、次のタスクを実行します。

1. デバイスをプロビジョニングします。

   Snort IPS 機能をインストールするデバイスを特定します。

2. ライセンスを取得します。

   Snort IPS 機能は、サービスを有効にするためにセキュリティライセンスを必要とするセキュリティパッケージでのみ使用できます。この機能は、Cisco IOS XE リリース 3.16.1S、3.17S、およびそれ以降のリリースで使用できます。

   （注） ライセンスの取得については、シスコ サポートにお問い合わせください。

3. Snort OVA ファイルをインストールします。
4. VirtualPortGroup のインターフェイスおよび仮想サービスを設定します。
5. Snort 仮想コンテナサービスをアクティブにします。
6. Snort IPS または IDS のモードとポリシーを設定します。
7. 外部アラートおよびログサーバまたは IOS syslog、あるいはその両方へのイベントのレポートを設定します。

8. 署名の更新方法を設定します。
9. 署名を更新します。
10. IPS をグローバルに、または必要なインターフェイスで有効にします。

# Snort OVA ファイルのインストール

OVA ファイルは、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。Snort IPS は仮想コンテナサービスとして使用できます。この OVA ファイルをルータにダウンロードし、**virtual-service install** CLI を使用してサービスをインストールする必要があります。

サービス OVA ファイルは、ルータにインストールされている Cisco IOS XE リリースイメージには付属していません。ただし、OVA ファイルはルータのフラッシュに事前にインストールされている場合があります。

セキュリティライセンスが付属した Cisco IOS XE イメージを使用する必要があります。OVA ファイルのインストール中に、セキュリティライセンスがチェックされ、ライセンスが存在しない場合はエラーが報告されます。

## 手順の概要

1. **enable**
2. **virtual-service install name** *virtual-service-name* **package** *file-url* **media** *file-system*
3. **show virtual-service list**

## 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**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **virtual-service install name** *virtual-service-name* **package** *file-url* **media** *file-system*<br>例：<br>`Device# virtual-service install name UTDIPS package harddisk:utd-ips-v102.ova media harddisk:` | デバイスの仮想サービスコンテナにアプリケーションをインストールします。<br>• 名前の長さは 20 文字です。ハイフン（-）は有効な文字ではありません。<br>• インストールする OVA パッケージの完全パスを指定する必要があります。<br>（注） OVA のインストールは、ハードディスクとブートフラッシュの両方で行えますが、OVA をインストールするのに推奨されるファイルシステムはハードディスクです。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **show virtual-service list**<br>例：<br>`Device# show virtual-service list` | 仮想サービスコンテナにインストールされているすべてのアプリケーションのインストールのステータスを表示します。 |

# VirtualPortGroup のインターフェイスおよび仮想サービスの設定

2 つの VirtualPortGroup インターフェイスと両方のインターフェイスのゲスト IP アドレスを設定する必要があります。ただし、 **vnic management GigabitEthernet0** コマンドを使用して管理インターフェイスを設定する場合は、最初の VirtualPortGroup インターフェイスのゲスト IP アドレスを設定しないでください。

（注） データトラフィック用の VirtualPortGroup インターフェイスは、プライベートまたはルーティング不可の IP アドレスを使用する必要があります。このインターフェイスには、IP アドレスの範囲として 192.0.2.0 / 30を 使用することを推奨します。

（注） Cisco IOS ソフトウェアイメージを XE 3.x バージョンから XE 16.2.1 に、または XE 16.2.1 から XE 3.x バージョンに変更する前に、デバイス上の仮想サービスごとに **virtual-service uninstall name [name]** コマンドを使用して仮想サービスをアンインストールします。仮想サービスの 1 つが ISR-WAAS サービスであり、**service waas enable** コマンドを使用してインストールされている場合は、**service waas disable** コマンドを使用します。

Cisco IOS ソフトウェアイメージの新しいバージョンでデバイスをアップグレードした後、仮想サービスを再インストールします。ISR-WAAS の場合は **service wass enable** コマンドを使用し、その他の仮想サービスの場合は **virtual-service install name [name] package [.ova file]** コマンドを使用します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *VirtualPortGroup number*
4. **ip address** *ip-address mask*
5. **exit**
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **exit**
9. **virtual-service** *name*
10. **profile** *profile-name*
11. **vnic gateway VirtualPortGroup** *interface-number*

12. **guest ip address** *ip-address*
13. **exit**
14. **vnic gateway VirtualPortGroup** *interface-number*
15. **guest ip address** *ip-address*
16. **exit**
17. **vnic management GigabitEthernet0**
18. **guest ip address** *ip-address*
19. **exit**
20. **activate**
21. **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**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Device# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **interface** *VirtualPortGroup number*<br>例：<br>`Device(config)# interface VirtualPortGroup 0` | インターフェイスを設定し、インターフェイス設定モードを開始します。<br>• VirtualPortGroup インターフェイスを設定します。このインターフェイスは、管理インターフェイスの GigabitEthernet0 が使用されていない場合に管理トラフィックに対して使用されます。 |
| ステップ 4 | **ip address** *ip-address mask*<br>例：<br>`Device(config-if)# ip address 10.1.1.1 255.255.255.252` | インターフェイスのプライマリ IP アドレスを設定します。このインターフェイスは、署名アップデートサーバおよび外部ログサーバにルーティング可能である必要があります。 |
| ステップ 5 | **exit**<br>例：<br>`Device(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 | **interface** *type number*<br>例：<br>`Device(config)# interface VirtualPortGroup 1` | インターフェイスを設定し、インターフェイス設定モードを開始します。<br>• VirtualPortGroup インターフェイスを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • このインターフェイスは、データトラフィックに使用されます。 |
| ステップ 7 | **ip address** *ip-address mask*<br>例：<br>`Device(config-if)# ip address 192.0.2.1 255.255.255.252` | インターフェイスのプライマリ IP アドレスを設定します。<br>• この IP アドレスは、外部ネットワークに対してルーティング不能である必要があります。<br>• IP アドレスは、推奨される 192.0.2.0/30 のサブネットから割り当てられます。 |
| ステップ 8 | **exit**<br>例：<br>`Device(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 9 | **virtual-service** *name*<br>例：<br>`Device(config)# virtual-service UTDIPS` | 仮想コンテナサービスを設定し、仮想サービス設定モードに入ります。<br>• *name* 引数は、仮想コンテナサービスを識別するために使用される論理名です。 |
| ステップ 10 | **profile** *profile-name*<br>例：<br>`Device(config-virt-serv)#profile high`<br>例：<br>`Device(config-virt-serv)#profile multi-tenancy` | （オプション）リソースプロファイルを設定します。リソースプロファイルを設定しない場合、仮想サービスはデフォルトのリソースプロファイルを使用してアクティブ化されます。オプションは、low、medium、high、および multi-tenancy です。（マルチテナントモードの場合（Cisco CSR 1000v のみ）、`profile multi-tenancy` コマンドを設定する必要があります。 |
| ステップ 11 | **vnic gateway VirtualPortGroup** *interface-number*<br>例：<br>`Device(config-virt-serv)# vnic gateway VirtualPortGroup 0` | 仮想コンテナサービスの仮想ネットワークインターフェイスカード（vNIC）のゲートウェイインターフェイスを作成し、vNIC ゲートウェイ インターフェイスを仮想ポートグループにマッピングして、仮想サービスの vNIC 設定モードに入ります。<br>• このコマンドで参照されるインターフェイスは、手順 3 で設定したインターフェイスである必要があります。このコマンドは、管理目的で使用されるインターフェイスをマッピングします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 12 | **guest ip address** *ip-address*<br>例：<br>`Device(config-virt-serv-vnic)# guest ip address 10.1.1.2` | （オプション）vNIC ゲートウェイ インターフェイスのゲスト vNIC アドレスを設定します。<br>• （注） 手順 17 で指定した **vnic management gigabitethernet0** コマンドが設定されていない場合にのみこのコマンドを設定します。 |
| ステップ 13 | **exit**<br>例：<br>`Device(config-virt-serv-vnic)# exit` | 仮想サービスの vNIC 設定モードを終了し、仮想サービス設定モードに戻ります。 |
| ステップ 14 | **vnic gateway VirtualPortGroup** *interface-number*<br>例：<br>`Device(config-virt-serv)# vnic gateway VirtualPortGroup 1` | 仮想コンテナサービスの vNIC ゲートウェイ インターフェイスを作成し、vNIC ゲートウェイ インターフェイスを仮想ポートグループにマッピングして、仮想サービスの vNIC 設定モードに入ります。<br>• このコマンドで参照されるインターフェイスは、手順 6 で設定したインターフェイスである必要があります。このコマンドは、Snort がユーザトラフィックのモニタリングに使用する仮想コンテナサービスのインターフェイスをマッピングします。 |
| ステップ 15 | **guest ip address** *ip-address*<br>例：<br>`Device(config-virt-serv-vnic)# guest ip address 192.0.2.2` | vNIC ゲートウェイ インターフェイスのゲスト vNIC アドレスを設定します。 |
| ステップ 16 | **exit**<br>例：<br>`Device(config-virt-serv-vnic)# exit` | 仮想サービスの vNIC 設定モードを終了し、仮想サービス設定モードに戻ります。 |
| ステップ 17 | **vnic management GigabitEthernet0**<br>例：<br>`Device(config-virt-serv)# vnic management GigabitEthernet0` | （オプション）GigabitEthernet インターフェイスを vNIC 管理インターフェイスとして設定します。<br>• 管理インターフェイスは、VirtualPortGroup インターフェイスまたは GibugitEthernet0 インターフェイスである必要があります。<br>• **vnic management GigabitEthernet0** コマンドを設定しない場合は、手順 12 で指定した **guest ip address** コマンドを設定する必要があります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 18 | **guest ip address** *ip-address*<br>例：<br>`Device(config-virt-serv-vnic)# guest ip address 209.165.201.1` | （オプション）vNIC 管理インターフェイスのゲスト vNIC アドレスを設定します。このアドレスは、管理インターフェイスおよび GigabitEthernet0 設定と同じサブネット内にある必要があります。 |
| ステップ 19 | **exit**<br>例：<br>`Device(config-virt-serv-vnic)# exit` | 仮想サービスの vNIC 設定モードを終了し、仮想サービス設定モードに戻ります。 |
| ステップ 20 | **activate**<br>例：<br>`Device(config-virt-serv)# activate` | 仮想コンテナサービスにインストールされたアプリケーションをアクティブにします。 |
| ステップ 21 | **end**<br>例：<br>`Device(config-virt-serv)# end` | 仮想サービス設定モードを終了し、特権 EXEC モードに戻ります。 |

# Snort IPS のグローバル設定

要件に基づいて、侵入防止システム（IPS）または侵入検知システム（IDS）の検査をグローバルレベルまたはインターフェイスで設定します。このタスクを実行して、デバイス上で IPS をグローバルに設定します。

（注） グローバルという用語は、対応しているすべてのインターフェイスで実行されている Snort IPS を意味します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **utd threat-inspection whitelist**
4. **generator id** *generator-id* **signature id** *signature-id* [**comment** *description*]
5. **exit**
6. **utd engine standard**
7. **logging** {**host** *hostname* | **syslog**}
8. **threat-inspection**
9. **threat** {**detection** | **protection** }
10. **policy** {**balanced** | **connectivity** | **security**}
11. **whitelist**
12. **signature update occur-at** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *hour minute*
13. **signature update server** {**cisco** | **url** *url* } [**username** *username* [**password** *password*]]

14. **logging level** {**alert** | **crit** | **debug** | **emerg** | **err** | **info** | **notice** | **warning**}
15. **exit**
16. **utd**
17. **redirect interface virtualPortGroup** *interface-number*
18. **all-interfaces**
19. **engine standard**
20. **fail close**
21. **exit**
22. **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**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Device# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **utd threat-inspection whitelist**<br>例：<br>`Device(config)# utd threat-inspection whitelist` | （オプション）UTD 許可リストの設定モードを有効にします。 |
| ステップ 4 | **generator id** *generator-id* **signature id** *signature-id* [**comment** *description*]<br>例：<br>`Device(config-utd-whitelist)# generator id 24 signature id 24245 comment traffic from branchoffice1` | 署名 ID を許可リストに表示するように設定します。<br>• 署名 IDは、抑制する必要があるアラートからコピーできます。<br>• 複数の署名 ID を設定できます。<br>• 許可リストに追加する必要がある署名 ID ごとに、この手順を繰り返します。 |
| ステップ 5 | **exit**<br>例：<br>`Device(config-utd-whitelist)# exit` | UTD 許可リストの設定モードを終了して、グローバル設定モードに戻ります。 |
| ステップ 6 | **utd engine standard**<br>例：<br>`Device(config)# utd engine standard` | 統合脅威防御（UTD）標準エンジンを設定し、UTD 標準エンジンの設定モードに入ります。 |
| ステップ 7 | **logging** {**host** *hostname* \| **syslog**}<br>例： | サーバへの緊急メッセージのロギングを有効にします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config-utd-eng-std)# logging host syslog.yourcompany.com` | |
| ステップ 8 | **threat-inspection**<br>例：<br>`Device(config-utd-eng-std)# threat-inspection` | Snort エンジンの脅威検知を設定します。 |
| ステップ 9 | **threat** {**detection** \| **protection** }<br>例：<br>`Device(config-utd-eng-std-insp)# threat protection` | 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。<br>• デフォルトは**detection**です。<br>• 侵入検知システム（IDS）を設定するには、**detection** キーワードを設定します。 |
| ステップ 10 | **policy** {**balanced** \| **connectivity** \| **security**}<br>例：<br>`Device(config-utd-eng-std-insp)# policy security` | Snort エンジンのセキュリティポリシーを設定します。<br>• デフォルトのポリシーオプションは **balanced** です。 |
| ステップ 11 | **whitelist**<br>例：<br>`Device(config-utd-eng-std-insp)# whitelist` | （オプション）UTD エンジンで許可リストを有効にします。 |
| ステップ 12 | **signature update occur-at** {**daily** \| **monthly** *day-of-month* \| **weekly** *day-of-week*} *hour minute*<br>例：<br>`Device(config-utd-eng-std-insp)# signature update occur-at daily 0 0` | 署名の更新間隔パラメータを設定します。この設定をすることで、午前0時に署名の更新がトリガーされます。 |
| ステップ 13 | **signature update server** {**cisco** \| **url** *url* } [**username** *username* [**password** *password*]]<br>例：<br>`Device(config-utd-eng-std-insp)# signature update server cisco username abcd password cisco123` | 署名更新サーバのパラメータを設定します。サーバの詳細で署名更新パラメータを指定する必要があります。署名の更新にCisco.comを使用する場合は、ユーザ名とパスワードを入力する必要があります。署名の更新にローカルサーバを使用する場合は、サーバ設定に基づいてユーザ名とパスワードを指定できます。 |
| ステップ 14 | **logging level** {**alert** \| **crit** \| **debug** \| **emerg** \| **err** \| **info** \| **notice** \| **warning**}<br>例：<br>`Device(config-utd-eng-std-insp)# logging level emerg` | ログレベルを有効にします。 |
| ステップ 15 | **exit**<br>例： | UTD標準エンジンの設定モードを終了して、グローバル設定モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config-utd-eng-std-insp)# exit` | |
| ステップ 16 | **utd**<br>例：<br>`Device(config)# utd` | 統合脅威防御（UTD）を有効にし、UTD 設定モードに入ります。 |
| ステップ 17 | **redirect interface virtualPortGroup** *interface-number*<br>例：<br>`Device(config-utd)# redirect interface virtualPortGroup 1` | （オプション）VirtualPortGroup インターフェイスにリダイレクトします。これはデータ トラフィック インターフェイスです。このインターフェイスを設定しない場合、インターフェイスは自動検出されます。 |
| ステップ 18 | **all-interfaces**<br>例：<br>`Device(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 19 | **engine standard**<br>例：<br>`Device(config-utd)# engine standard` | 統合脅威防御（UTD）エンジンを設定し、標準エンジンの設定モードに入ります。 |
| ステップ 20 | **fail close**<br>例：<br>`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。 |
| ステップ 21 | **exit**<br>例：<br>`Device(config-eng-std)# exit` | 標準エンジンの設定モードを終了して、グローバル設定モードに戻ります。 |
| ステップ 22 | **end**<br>例：<br>`Device(config-utd)# end` | UTD 設定モードを終了して、グローバル設定モードに戻ります。 |

# Snort IDS 検知のグローバル設定

要件に基づいて、侵入防止システム（IPS）または侵入検知システム（IDS）検査をグローバルレベルまたはインターフェイスレベルで設定します。インターフェイスごとに IDS を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **utd enable**
5. **exit**
6. 検査が必要な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。
7. **utd threat-inspection whitelist**
8. **generator id** *generator-id* **signature id** *signature-id* [**comment** *description*]
9. **exit**
10. **utd engine standard**
11. **logging** {**host** *hostname* | **syslog**}
12. **threat-inspection**
13. **threat** {**detection** | **protection** }
14. **policy** {**balanced** | **connectivity** | **security**}
15. **whitelist**
16. **signature update occur-at** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *hour minute*
17. **signature update server** {**cisco** | **url** *url*} [**username** *username* [**password** *password*]]
18. **logging level** {**alert** | **crit** | **debug** | **emerg** | **err** | **info** | **notice** | **warning**}
19. **exit**
20. **utd**
21. **redirect interface virtualPortGroup** *interface-number*
22. **engine standard**
23. **fail close**
24. **exit**
25. **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**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Device# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **interface** *type number*<br>例：<br>`Device(config)# interface gigabitethernet 0/0/0` | インターフェイスを設定し、インターフェイス設定モードを開始します。 |
| ステップ 4 | **utd enable**<br>例： | 統合脅威防御（UTD）を有効にします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config-if)# utd enable` | |
| ステップ 5 | **exit**<br>例：<br>`Device(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 | 検査が必要な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。 | – |
| ステップ 7 | **utd threat-inspection whitelist**<br>例：<br>`Device(config)# utd threat-inspection whitelist` | （オプション）UTD 許可リストの設定モードを有効にします。 |
| ステップ 8 | **generator id** *generator-id* **signature id** *signature-id* [**comment** *description*]<br>例：<br>`Device(config-utd-whitelist)# generator id 24 signature id 24245 comment traffic from branchoffice1` | 署名 ID を許可リストで表示するように設定します。<br>• 署名 IDは、抑制する必要があるアラートからコピーできます。<br>• 複数の署名 ID を設定できます。<br>• 許可リストに表示する必要がある署名 ID ごとに、この手順を繰り返します。 |
| ステップ 9 | **exit**<br>例：<br>`Device(config-utd-whitelist)# exit` | UTD 許可リストの設定モードを終了して、グローバル設定モードに戻ります。 |
| ステップ 10 | **utd engine standard**<br>例：<br>`Device(config)# utd engine standard` | 統合脅威防御（UTD）標準エンジンを設定し、UTD 標準エンジンの設定モードに入ります。 |
| ステップ 11 | **logging** {**host** *hostname* \| **syslog**}<br>例：<br>`Device(config-utd-eng-std)# logging syslog` | IOSd syslog への重要なメッセージのロギングを有効にします。 |
| ステップ 12 | **threat-inspection**<br>例：<br>`Device(config-utd-eng-std)# threat-inspection` | Snort エンジンの脅威検知を設定します。 |
| ステップ 13 | **threat** {**detection** \| **protection** }<br>例：<br>`Device(config-utd-eng-std-insp)# threat detection` | 脅威防止または侵入検知システム（IDS）を Snort センサーの動作モードとして設定します。<br>• 侵入防止システム（IPS）を設定するには、**protection** キーワードを設定します。 |
| ステップ 14 | **policy** {**balanced** \| **connectivity** \| **security**}<br>例： | Snort センサーのセキュリティポリシーを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config-utd-eng-std-insp)# policy balanced` | |
| ステップ 15 | **whitelist**<br>例：<br>`Device(config-utd-eng-std-insp)# whitelist` | （オプション）トラフィックの許可リストを有効にします。 |
| ステップ 16 | **signature update occur-at** {**daily** \| **monthly** *day-of-month* \| **weekly** *day-of-week*} *hour minute*<br>例：<br>`Device(config-utd-eng-std-insp)# signature update occur-at daily 0 0` | 署名の更新間隔パラメータを設定します。この設定をすることで、午前0時に署名の更新がトリガーされます。 |
| ステップ 17 | **signature update server** {**cisco** \| **url** *url*} [**username** *username* [**password** *password*]]<br>例：<br>`Device(config-utd-eng-std-insp)# signature update server cisco username abcd password cisco123` | 署名更新サーバのパラメータを設定します。サーバの詳細で署名更新パラメータを指定する必要があります。署名の更新にCisco.comを使用する場合は、ユーザ名とパスワードを入力する必要があります。署名の更新にローカルサーバを使用する場合は、サーバ設定に基づいてユーザ名とパスワードを指定できます。 |
| ステップ 18 | **logging level** {**alert** \| **crit** \| **debug** \| **emerg** \| **err** \| **info** \| **notice** \| **warning**}<br>例：<br>`Device(config-utd-eng-std-insp)# logging level crit` | ログレベルを有効にします。 |
| ステップ 19 | **exit**<br>例：<br>`Device(config-utd-eng-std-insp)# exit` | UTD標準エンジンの設定モードを終了して、グローバル設定モードに戻ります。 |
| ステップ 20 | **utd**<br>例：<br>`Device(config)# utd` | 統合脅威防御（UTD）を有効にし、UTD 設定モードに入ります。 |
| ステップ 21 | **redirect interface virtualPortGroup** *interface-number*<br>例：<br>`Device(config-utd)# redirect interface virtualPortGroup 1` | （オプション）VirtualPortGroup インターフェイスにリダイレクトします。これはデータ トラフィック インターフェイスです。このインターフェイスを設定しない場合、インターフェイスは自動検出されます。 |
| ステップ 22 | **engine standard**<br>例：<br>`Device(config-utd)# engine standard` | 統合脅威防御（UTD）エンジンを設定し、標準エンジンの設定モードに入ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 23 | **fail close**<br>例：<br>`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。 |
| ステップ 24 | **exit**<br>例：<br>`Device(config-eng-std)# exit` | 標準エンジンの設定モードを終了して、グローバル設定モードに戻ります。 |
| ステップ 25 | **end**<br>例：<br>`Device(config-utd)# end` | 設定モードを終了し、EXEC モードに戻ります。 |

## アクティブな署名のリストの表示

アクティブな署名は、Snort IDS または IPS に脅威に対するアクションを実行するように指示するものです。トラフィックがアクティブな署名のいずれかと一致した場合、Snort コンテナは IDS モードでアラートをトリガーし、IPS モードでトラフィックをドロップします。

**utd threat-inspection signature active-list write-to bootflash: file name** コマンドは、アクティブな署名のリストと、アクティブな署名、ドロップ署名、およびアラート署名の合計数のサマリーを表示します。

# Snort IPS の設定例

## 例：VirtualPortGroup インターフェイスおよび仮想サービスの設定

```
Device# configure terminal
Device(config)# interface VirtualPortGroup 0
Device(config-if)# ip address 10.1.1.1 255.255.255.252
Device(config-if)# exit
Device(config)# interface VirtualPortGroup 1
Device(config-if)# ip address 192.0.2.1 255.255.255.252
Device(config-if)# exit
Device(config)# virtual-service UTDIPS
Device(config-virt-serv)# vnic gateway VirtualPortGroup 0
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# vnic gateway VirtualPortGroup 1
Device(config-virt-serv-vnic)# guest ip address 192.0.2.2
Device(config-virt-serv-vnic)# exit
```

```
Device(config-virt-serv)# vnic management GigabitEthernet0
Device(config-virt-serv-vnic)# guest ip address 209.165.201.1
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# activate
Device(config-virt-serv-vnic)# end
```

# 例：異なるリソースプロファイルの設定

```
Device# configure terminal
Device(config)# virtual-service UTDIPS
Device(config-virt-serv)# no activate
Device(config-virt-serv)# end
Device# virtual-service uninstall name UTDIPS
Device# configure terminal
Device(config)# virtual-service UTDIPS
Device(config-virt-serv)# profile medium
Device(config-virt-serv)# end
Device# virtual-service install name UTDIPS package:utd.ova
Device# configure terminal
Device(config)# virtual-service UTDIPS
Device(config-virt-serv)# activate
Device(config-virt-serv)# end
```

# 例：Snort IPS のグローバル設定

次に、デバイス上で侵入防止システム（IPS）をグローバルに設定する例を示します。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# threat protection
Device(config-utd-eng-std-insp)# policy security
Device(config-utd-eng-std)# exit
Device(config)# utd
Device(config-utd)# all-interfaces
Device(config-utd)# engine standard
Device(config-utd-whitelist)# end
Device#
```

# 例：インターフェイスごとの Snort IPS 検査の設定

次に、インターフェイスごとにSnort侵入検知システム（IDS）を設定する例を示します。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# threat detection
Device(config-utd-eng-std-insp)# policy security
Device(config-utd-eng-std)# exit
```

```
Device(config)# utd
Device(config-utd)# engine standard
Device(config-eng-std)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# utd enable
Device(config-if)# exit
```

# 例：インバウンドインターフェイスとアウトバウンドインターフェイスの両方での VRF を使用した UTD の設定

```
Device# configure terminal
Device(config)# vrf definition VRF1
Device(config-vrf)# rd 100:1
Device(config-vrf)# route-target export 100:1
Device(config-vrf)# route-target import 100:1
Device(config-vrf)# route-target import 100:2
!
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit
!
Device(config-vrf-af)# vrf definition VRF2
Device(config-vrf)# rd 100:2
Device(config-vrf)# route-target export 100:2
Device(config-vrf)# route-target import 100:2
Device(config-vrf)# route-target import 100:1
!
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit
!
Device(config-vrf)# interface VirtualPortGroup0
Device(config-if)# ip address 192.0.2.1 255.255.255.252
Device(config-if)# no mop enabled
Device(config-if)# no mop sysid
!
Device(config-if)# interface VirtualPortGroup1
Device(config-if)# ip address 192.0.2.5 255.255.255.252
Device(config-if)# no mop enabled
Device(config-if)# no mop sysid
!
Device(config-if)# interface GigabitEthernet0/0/2
Device(config-if)# vrf forwarding VRF1
Device(config-if-vrf)# ip address 192.1.1.5 255.255.255.0
Device(config-if-vrf)# ipv6 address A000::1/64
!
Device(config-if)# interface GigabitEthernet0/0/3
Device(config-if)# vrf forwarding VRF2
Device(config-if-vrf)# ip address 192.1.1.5 255.255.255.0
Device(config-if-vrf)# ipv6 address B000::1/64
!
Device(config-if-vrf)# router bgp 100
Device(config-if-vrf)# bgp log-neighbor-changes
!
Device(config-vrf)# address-family ipv4 vrf VRF1
Device(config-vrf-af)# redistribute connected
```

```
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6 vrf VRF1
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv4 vrf VRF2
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6 vrf VRF2
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config)# utd
Device(config-utd)# all-interfaces
Device(config-utd)# engine standard
Device(config-utd)# exit

Device(config)# utd engine standard
Device(config-utd-eng-std)# logging syslog
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# threat protection
Device(config-utd-engstd-insp)# policy security
Device(config-utd-engstd-insp)# exist
Device(config-utd-eng-std)# exit
!
Device(config)# virtual-service utd
Device(config-virt-serv)# profile low
Device(config-virt-serv)# vnic gateway VirtualPortGroup0
Device(config-virt-serv-vnic)# guest ip address 192.0.2.2
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# vnic gateway VirtualPortGroup1
Device(config-virt-serv-vnic)# guest ip address 192.0.2.6
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# activate

UTD Snort IPS Drop Log
============================
2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**]
[1:30561:1] BLACKLIST DNS request for known malware
domain domai.ddns2.biz - Win.Trojan.Beebone [**]
[Classification: A Network Trojan was Detected]
[Priority: 1] [VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53
```

# 例：IOS Syslog のロギングの設定

次に、デバイスのログレベルを使用して IOS syslog のロギングを設定する例を示します。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# logging syslog
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# logging level debug
Device(config-utd-eng-std-insp)# end
Device#
```

# 例：中央集中型ログサーバへのロギングの設定

次の例は、中央集中型ログサーバへのロギングの設定方法を示しています。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std-insp)# logging host syslog.yourcompany.com
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# logging level info
Device(config-utd-eng-std-insp)# end
Device#
```

# 例：Cisco サーバからの署名更新の設定

次の例は、Cisco サーバから署名の更新を設定する方法を示しています。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# signature update server cisco username CCOuser password
 passwd123
Device(config-utd-eng-std-insp)# end
Device#
```

（注） DNS が Cisco サーバから署名をダウンロードするように設定されていることを確認します。

# 例：ローカルサーバからの署名更新の設定

次の例は、ローカルサーバから署名の更新を設定する方法を示しています。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# signature update server url http://192.168.1.2/sig-1.pkg
Device(config-utd-eng-std-insp)# end
Device#
```

# 例：自動署名更新の設定

次の例は、サーバで自動署名更新を設定する方法を示しています。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# signature update occur-at daily 0 0
Device(config-utd-eng-std-insp)# signature update server cisco username abcd password
cisco123
```

```
Device(config-utd-eng-std-insp)# end
Device#
```

# 例：手動による署名の更新の実行

次の例は、さまざまな方法で手動で署名を更新する方法を示しています。

```
Device# utd threat-inspection signature update
```

既存のサーバ設定をダウンロードするか、既存のサーバ設定を使用して設定された明示的なサーバ情報を取得します。これらのコマンドにより、次の設定を使用して手動で署名更新が実行されます。

```
Device# show utd engine standard threat-inspection signature update status

Current signature package version: 2983.4.s
Current signature package name: UTD-STD-SIGNATURE-2983-4-S.pkg
Previous signature package version: 29.0.c
----------------------------------------
Last update status: Successful
----------------------------------------
Last successful update time: Mon Aug  7 02:02:32 2017 UTC
Last successful update method: Manual
Last successful update server: cisco
Last successful update speed: 3022328 bytes in 25 secs
----------------------------------------
Last failed update time: Mon Aug  7 01:53:21 2017 UTC
Last failed update method: Manual
Last failed update server: cisco
Last failed update reason: ('Connection aborted.', gaierror(-2, 'Name or service hnot
known'))
----------------------------------------
Last attempted update time: Mon Aug  7 02:02:32 2017 UTC
Last attempted update method: Manual
Last attempted update server: cisco
----------------------------------------
Total num of updates successful: 1
Num of attempts successful: 1
Num of attempts failed: 3
Total num of attempts: 4
----------------------------------------
Next update scheduled at: None
----------------------------------------
Current status: Idle


Device# utd threat-inspection signature update server cisco username ccouser password
passwd123

Device# utd threat-inspection signature update server url http://192.168.1.2/sig-1.pkg
```

# 例：署名のホワイトリストの設定

次の例は、署名のホワイトリストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# utd threat-inspection whitelist
Device(config-utd-whitelist)# utd-whitelist)# generator id 1 signature id 23456 comment
```

```
 "traffic from client x"
Device(config-utd-whitelist)# exit
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# whitelist
Device(config-utd-eng-std-insp)# end
Device#
```

（注） ホワイトリストの署名 ID が設定されると、Snort はフローがアラートやドロップなしでデバイスを通過できるようにします。

# アクティブな署名の表示例

## 例：接続ポリシーを使用したアクティブな署名の表示

```
Device# utd threat-inspection signature active-list write-to bootflash:siglist_connectivity
Device# more bootflash:siglist_connectivity
================================================================================
Signature Package Version: 2982.1.s
Signature Ruleset: Connectivity
Total no. of active signatures: 581
Total no. of drop signatures: 452
Total no. of alert signatures: 129

For more details of each signature please go to www.snort.org/rule_docs to lookup
================================================================================
List of Active Signatures:
--------------------------
<snipped>
```

## 例：バランスの取れたポリシーを使用したアクティブな署名の表示

```
Device# utd threat-inspection signature active-list write-to bootflash:siglist_balanced
Device# more bootflash:siglist_balanced
================================================================================
Signature Package Version: 2982.1.s
Signature Ruleset: Balanced
Total no. of active signatures: 7884
Total no. of drop signatures: 7389
Total no. of alert signatures: 495

For more details of each signature please go to www.snort.org/rule_docs to lookup
================================================================================

List of Active Signatures:
--------------------------
<snipped>
```

# 例：セキュリティポリシーを使用したアクティブな署名の表示

```
Device# utd threat-inspection signature active-list write-to bootflash:siglist_security
Device# more bootflash:siglist_security
================================================================================
Signature Package Version: 2982.1.s
Signature Ruleset: Security
Total no. of active signatures: 11224
Total no. of drop signatures: 10220
Total no. of alert signatures: 1004

For more details of each signature please go to www.snort.org/rule_docs to lookup
================================================================================

List of Active Signatures:
--------------------------
<snipped>
```

# 統合型 Snort IPS 設定の確認

次のコマンドを使用して、設定をトラブルシューティングします。

## 手順の概要

1. **enable**
2. **show virtual-service list**
3. **show virtual-service detail**
4. **show service-insertion type utd service-node-group**
5. **show service-insertion type utd service-context**
6. **show utd engine standard config**
7. **show utd engine standard status**
8. **show utd engine standard  threat-inspection signature update status**
9. **show utd engine standard logging events**
10. **clear utd engine standard logging events**
11. **show platform hardware qfp active feature utd config**
12. **show platform software utd global**
13. **show platform software utd interfaces**
14. **show platform hardware qfp active feature utd stats**
15. **show utd engine standard statistics daq all**

## 手順の詳細

### ステップ 1　**enable**

例：

```
Device> 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　show virtual-service list

仮想サービスコンテナ上のすべてのアプリケーションのインストールのステータスを表示します。

**例**：

```
Device# show virtual-service list

Virtual Service List:


Name                     Status              Package Name
------------------------------------------------------------------------------
UTDIPS                   Activated           utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
```

### ステップ 3　show virtual-service detail

デバイスの仮想サービスコンテナにインストールされているアプリケーションによって使用されるリソースを表示します。

**例**：

```
Device# show virtual-service detail


Device#show virtual-service detail
Virtual service UTDIPS detail
  State                : Activated
  Owner                : IOSd
  Package information
    Name               : utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Path               : bootflash:/utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Application
      Name             : UTD-Snort-Feature
      Installed version : 1.0.1_SV2982_XE_16_3
      Description      : Unified Threat Defense
    Signing
      Key type         : Cisco development key
      Method           : SHA-1
    Licensing
      Name             : Not Available
      Version          : Not Available

  Detailed guest status

------------------------------------------------------------------------
Process               Status            Uptime           # of restarts
------------------------------------------------------------------------
climgr                 UP         0Y 0W 0D  0: 0:35        1
logger                 UP         0Y 0W 0D  0: 0: 4        0
snort_1                UP         0Y 0W 0D  0: 0: 4        0
Network stats:
eth0: RX  packets:43, TX  packets:6
eth1: RX  packets:8, TX  packets:6

Coredump file(s): lost+found

  Activated profile name: None
  Resource reservation
    Disk               : 736 MB
    Memory             : 1024 MB
    CPU                : 25% system CPU
```

```
  Attached devices
    Type              Name        Alias
    ---------------------------------------------
    NIC               ieobc_1     ieobc
    NIC               dp_1_0      net2
    NIC               dp_1_1      net3
    NIC               mgmt_1      mgmt
    Disk              _rootfs
    Disk              /opt/var
    Disk              /opt/var/c
    Serial/shell                  serial0
    Serial/aux                    serial1
    Serial/Syslog                 serial2
    Serial/Trace                  serial3
    Watchdog          watchdog-2

  Network interfaces
    MAC address             Attached to interface
    ------------------------------------------------------
    54:0E:00:0B:0C:02       ieobc_1
    A4:4C:11:9E:13:8D       VirtualPortGroup0
    A4:4C:11:9E:13:8C       VirtualPortGroup1
    A4:4C:11:9E:13:8B       mgmt_1

  Guest interface
  ---
  Interface: eth2
  ip address: 48.0.0.2/24
Interface: eth1
  ip address: 47.0.0.2/24

  ---

  Guest routes
  ---
  Address/Mask                        Next Hop                          Intf.
-------------------------------------------------------------------------------
0.0.0.0/0                           48.0.0.1                          eth2
0.0.0.0/0                           47.0.0.1                          eth1

  ---

  Resource admission (without profile) : passed
    Disk space    : 710MB
    Memory        : 1024MB
    CPU           : 25% system CPU
    VCPUs         : Not specified
```

### ステップ 4　show service-insertion type utd service-node-group

サービスノードグループのステータスを表示します。

例：

```
Device# show service-insertion type utd service-node-group

Service Node Group name : utd_sng_1
Service Context : utd/1
Member Service Node count : 1


Service Node (SN) : 30.30.30.2
Auto discovered : No
```

```
SN belongs to SNG : utd_sng_1
Current status of SN : Alive
Time current status was reached : Tue Jul 26 11:57:48 2016

Cluster protocol VPATH version : 1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1469514497
Cluster protocol last received sequence number: 1464
Cluster protocol last received ack number : 1469514496
```

### ステップ 5 show service-insertion type utd service-context

AppNav およびサービスノードビューを表示します。

**例**：

```
Device# show service-insertion type utd service-context

Service Context : utd/1
Cluster protocol VPATH version : 1
Time service context was enabled : Tue Jul 26 11:57:47 2016
Current FSM state : Operational
Time FSM entered current state : Tue Jul 26 11:57:58 2016
Last FSM state : Converging
Time FSM entered last state : Tue Jul 26 11:57:47 2016
Cluster operational state : Operational

Stable AppNav controller View:
30.30.30.1

Stable SN View:
30.30.30.2

Current AppNav Controller View:
30.30.30.1

Current SN View:
30.30.30.2
```

### ステップ 6 show utd engine standard config

統合脅威防御（UTD）の設定を表示します。

**例**：

```
Device# show utd engine standard config


UTD Engine Standard Configuration:
  Operation Mode : Intrusion Prevention
  Policy         : Security

Signature Update:
  Server    : cisco
  User Name : ccouser
  Password  : YEX^SH\fhdOeEGaOBIQAIcOVLgaVGf
  Occurs-at : weekly ;  Days:0 ; Hour: 23; Minute: 50

Logging:
  Server    :   IOS Syslog; 10.104.49.223
  Level     : debug

Whitelist Signature IDs:
```

```
  28878
```

### ステップ 7　show utd engine standard status

UTD エンジンのステータスを表示します。

例：

```
Device# show utd engine standard status

Profile : High
System memory :
Usage : 8.00 %
Status : Green
Number of engines : 4

Engine Running CFT flows Health Reason
======================================================
Engine(#1): Yes 0 Green None
Engine(#2): Yes 0 Green None
Engine(#3): Yes 0 Green None
Engine(#4): Yes 0 Green None
======================================================

Overall system status: Green

Signature update status:
========================
Current signature package version: 2983.4.s
Last update status: Successful
Last successful update time: Mon Aug  7 02:02:32 2017 UTC
Last failed update time: Mon Aug  7 01:53:21 2017 UTC
Last failed update reason: ('Connection aborted.', gaierror(-2, 'Name or service not known'))
Next update scheduled at: None
Current status: Idle
```

### ステップ 8　show utd engine standard  threat-inspection signature update status

署名更新プロセスのステータスを表示します。

例：

```
Device# show utd engine standard threat-inspection signature update status

Current signature package version: 2983.4.s
Current signature package name: UTD-STD-SIGNATURE-2983-4-S.pkg
Previous signature package version: 29.0.c
----------------------------------------
Last update status: Successful
----------------------------------------
Last successful update time: Mon Aug  7 02:02:32 2017 UTC
Last successful update method: Manual
Last successful update server: cisco
Last successful update speed: 3022328 bytes in 25 secs
----------------------------------------
Last failed update time: Mon Aug  7 01:53:21 2017 UTC
Last failed update method: Manual
Last failed update server: cisco
Last failed update reason: ('Connection aborted.', gaierror(-2, 'Name or service hnot known'))
----------------------------------------
Last attempted update time: Mon Aug  7 02:02:32 2017 UTC
Last attempted update method: Manual
```

```
Last attempted update server: cisco
---------------------------------------
Total num of updates successful: 1
Num of attempts successful: 1
Num of attempts failed: 3
Total num of attempts: 4
---------------------------------------
Next update scheduled at: None
---------------------------------------
Current status: Idle
```

**ステップ 9　show utd engine standard logging events**

Snort センサーからのログイベントを表示します。

**例**：

```
Device# show utd engine standard logging events

2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53
2016/06/13-14:32:21.524988 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} a000:0:0:0:0:0:0:10:59964 -> b000:0:0:0:0:0:0:10:53
```

**ステップ 10　clear utd engine standard logging events**

**例**：

```
Device# clear utd engine standard logging events
```

Snort センサーからのログイベントをクリアします。

**ステップ 11　show platform hardware qfp active feature utd config**

サービスノードの正常性に関する情報を表示します。

**例**：

```
Device# show platform hardware qfp active feature utd config

Global configuration
NAT64: disabled
SN threads: 12
CFT inst_id 0 feat id 1 fo id 1 chunk id 8
Context Id: 0, Name: Base Security Ctx
Ctx Flags: (0x60000)
Engine: Standard
SN Redirect Mode : Fail-open, Divert
Threat-inspection: Enabled, Mode: IDS
Domain Filtering : Not Enabled
URL Filtering : Not Enabled
SN Health: Green
```

**ステップ 12　show platform software utd global**

UTD が有効になっているインターフェイスを表示します。

例：

```
Device# show platform software utd global

UTD Global state
Engine               : Standard
Global Inspection    : Enabled
Operational Mode     : Intrusion Prevention
Fail Policy          : Fail-open
Container techonlogy : LXC
Redirect interface   : VirtualPortGroup1
UTD interfaces
All dataplane interfaces
```

### ステップ 13 show platform software utd interfaces

すべてのインターフェイスに関する情報を表示します。

例：

```
Device# show platform software utd interfaces

UTD interfaces
All dataplane interfaces
```

### ステップ 14 show platform hardware qfp active feature utd stats

データプレーンの UTD 統計情報を表示します。

例：

```
Device# show platform hardware qfp active feature utd stats

Security Context:    Id:0    Name: Base Security Ctx

Summary Statistics:
Pkts entered policy feature                        pkt                 228
                                                   byt               31083

Drop Statistics:

Service Node flagged flow for dropping                                  48
Service Node not healthy                                                62

General Statistics:

Non Diverted Pkts to/from divert interface                            32913
Inspection skipped - UTD policy not applicable                        48892
Policy already inspected                                               2226
Pkts Skipped - L2 adjacency glean                                         1
Pkts Skipped - For Us                                                    67
Pkts Skipped - New pkt from RP                                          102
Response Packet Seen                                                    891
Feature memory allocations                                              891
Feature memory free                                                     891
Feature Object Delete                                                   863

Service Node Statistics:
SN Health: Green
SN down                                                                  85
SN health green                                                          47
SN health red                                                            13
```

```
Diversion Statistics
redirect                                                                2226
encaps                                                                  2226
decaps                                                                  2298
reinject                                                                2250
decaps: Could not locate flow                                             72
Redirect failed, SN unhealthy                                             62
Service Node requested flow bypass drop                                   48
```

### ステップ 15　show utd engine standard statistics daq all

サービスプレーンのデータ収集（DAQ）の統計情報を表示します。

**例**：

```
Device# show utd engine standard statistics daq all

IOS-XE DAQ Counters(Engine #1):
--------------------------------
Frames received                         :0
Bytes received                          :0
RX frames released                      :0
Packets after vPath decap               :0
Bytes after vPath decap                 :0
Packets before vPath decap              :0
Bytes before vPath decap                :0
Frames transmitted                      :0
Bytes transmitted                       :0

Memory allocation                       :2
Memory free                             :0
Merged packet buffer allocation         :0
Merged packet buffer free               :0

VPL buffer allocation                   :0
VPL buffer free                         :0
VPL buffer expand                       :0
VPL buffer merge                        :0
VPL buffer split                        :0
VPL packet incomplete                   :0

VPL API error                           :0
CFT API error                           :0
Internal error                          :0
External error                          :0
Memory error                            :0
Timer error                             :0

Kernel frames received                  :0
Kernel frames dropped                   :0

FO cached via timer                     :0
Cached fo used                          :0
Cached fo freed                         :0
FO not found                            :0
CFT full packets                        :0


VPL Stats(Engine #1):
```

---

# Cisco Prime CLI テンプレートを使用した Snort IPS の導入

Cisco Prime CLI テンプレートを使用して、Snort IPS 導入をプロビジョニングすることができます。Cisco Prime CLI テンプレートを使用すると、Snort IPS 導入を容易にプロビジョニングできます。Cisco Prime CLI テンプレートを Snort IPS 導入のプロビジョニングに使用するには、次の手順を実行します。

**ステップ 1** システムで実行されている IOS XE バージョンに対応する Prime テンプレートをソフトウェアのダウンロードページからダウンロードします。

**ステップ 2** このファイルが圧縮されている場合は解凍します。

**ステップ 3** Prime から、[Configuration] > [Templates] > [Features and Technologies] の順に選び、[CLI Templates] を選択します。

**ステップ 4** [Import] をクリックします。

**ステップ 5** テンプレートのインポート先フォルダを選択し、[Select Templates] をクリックして、先ほどダウンロードしたテンプレートを選択してインポートします。

次の Snort IPS CLI テンプレートを使用できます。

- Copy OVA to Device：このテンプレートを使用して、Snort IPS OVA ファイルをルータのファイルシステムにコピーします。
- Delete OVA：このテンプレートを使用して、コピーした Snort IPS OVA ファイルをルータのファイルシステムから削除します。
- Dynamic NAT：ダイナミック NAT（ネットワークアドレス変換）が環境内で設定されており、Snort IPS 管理インターフェイス IP 用に変更する必要がある NAT 変換を選択するためにアクセスリストを使用する場合は、このテンプレートを使用します。
- Dynamic NAT Cleanup：このテンプレートを使用して、Snort IPS の NAT 設定を削除します。
- Dynamic PAT：環境内でダイナミック PAT（ポートアドレス変換）が設定されており、Snort IPS 管理インターフェイスIP用に変更する必要のある PAT 変換を選択するためにアクセスリストを使用する場合は、このテンプレートを使用します。
- Dynamic NAT Cleanup：このテンプレートを使用して、Snort IPS の PAT 設定を削除します。
- IP Unnumbered：このテンプレートを使用して、Snort IPS および IP 番号なしの導入に必要な仮想サービスを設定します。
- IP Unnumbered Cleanup：このテンプレートを使用して、IP 番号なしで設定された Snort IPS 管理インターフェイスを削除します。

- Management Interface：Snort IPS 管理トラフィックのルーティングにシステム管理インターフェイス（GigabitEthernet0 など）を使用する場合は、このテンプレートを使用します。
- Management Interface Cleanup：このテンプレートを使用して、Snort IPS 管理トラフィックをルーティングするために設定されたシステム管理インターフェイス（GigabitEthernet0 など）を削除します。
- Static NAT：このテンプレートを使用して、Snort IPS および既存の静的 NAT の導入に必要な仮想サービスを設定します。
- Static NAT Cleanup：このテンプレートを使用して、静的 NAT の導入で設定された Snort IPS を削除します。
- Upgrade OVA：このテンプレートを使用して、Snort IPS の OVA ファイルをアップグレードします。

# IOx コンテナへの移行

ここでは、Cisco 1000 シリーズサービス統合型ルータ（ISR）での UTD 対応を拡張するための、Cisco IOx および IOx への UTD の移行について説明します。Cisco IOx では Cisco IOS と Linux OS が組み合わされており、安全性の高いネットワークを実現します。

## Cisco IOx について

Cisco IOx は、さまざまな Cisco プラットフォームにおける各種アプリケーションに統一された一貫性のあるホスティング機能を提供するアプリケーション プラットフォームです。このプラットフォームは、ネットワーキング オペレーティング システム（Cisco IOS）とオープンソースのプラットフォーム（Linux）を統合し、ネットワーク上のカスタムアプリケーションとインターフェイスを実現します。

仮想サービス コンテナはデバイスの仮想化環境です。仮想マシン（VM）、仮想サービス、またはコンテナとも呼ばれます。仮想サービス コンテナ内にアプリケーションをインストールできます。このアプリケーションは、デバイスのオペレーティング システムの仮想サービス コンテナ内で稼動します。アプリケーションは、拡張子 .ova を持つ tar ファイルである Open Virtual Application（OVA）として提供されます。OVA パッケージは、コマンドラインのインターフェイスを介してデバイスにインストールされ、有効化されます。オープンフローの Cisco プラグインは、仮想サービスコンテナ内に導入できるアプリケーションの一例です。

UTD OVA をホストするために使用される仮想サービスコンテナのインフラストラクチャは、Cisco 1100 シリーズ ISR では対応していません。現在、UTD は両方のコンテナに対応しています。ただし、OVA コンテナ機能は Cisco IOS XE Gibrafilter 16.10 のリリースでは対応していますが、それ以降のリリースでは対応していません。

# 仮想サービスコンテナから IOx へのアップグレード

OVA ファイルは、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。Snort IPS は仮想コンテナサービスとして使用できます。この OVA ファイルをデバイスにダウンロードし、**virtual-service install** CLI を使用してサービスをインストールする必要があります。

UTD IOx インフラストラクチャの場合、IOx ベースの OVA は IOx CLI コマンドを使用してインストールします。インストールする前に、グローバル設定モードでIOx環境を開始します。

IOx ベースの OVA は TAR ファイルと呼ばれます。セキュリティライセンスが付属した Cisco IOS XE イメージを使用する必要があります。OVA ファイルのインストール中に、セキュリティライセンスがチェックされ、ライセンスが存在しない場合はエラーが報告されます。

仮想サービスから IOx コンテナにアップグレードするには、次の手順を実行します。

**ステップ 1** **no activate**

例：

```
Device# configure terminal
Device (config)# virtual-service utd
Device (config-virt-serv)# no activate
Device (config-virt-serv)# exit
Device (config)# no virtual-service utd
```

仮想マネージャベースの仮想サービスのインスタンスを非アクティブにします。

**ステップ 2** **show virtual-service list**

例：

```
Device# show virtual-service list
```

仮想サービスコンテナにインストールされているすべてのアプリケーションのステータスを表示します。仮想サービスインスタンスが非アクティブになっていることを確認します。

**ステップ 3** **virtual-service uninstall name** *virtual-service instance*

例：

```
Device# virtual-service uninstall name utd
```

仮想マネージャベースの仮想サービスインスタンスをアンインストールします。**show virtual-service list** コマンドを実行したときに、仮想サービスインスタンスが表示されないことを確認します。

**ステップ 4** **iox**

例：

```
Device# configure terminal
Device (config)# iox
Device (config)# end
```

IOx環境をグローバル設定モードで開始します。

**ステップ 5** **app-hosting install appid** *name* **package** *bootflash:<tarfile>*

例：

```
Device# app-hosting install appid UTD package bootflash:utd.tar
Device#
```

Iox ベースの OVA tar ファイルをデバイスにコピーしてインストールします。

**ステップ 6** **show app-hosting list**

例：

```
Device# show app-hosting list
App id                                   State
---------------------------------------------------------
UTD                                      DEPLOYED
Device#
```

インストールのステータスを表示します。アプリケーションが展開されていることを確認します。

**ステップ 7** **app-hosting activate appid** *name*

例：

```
Device# app-hosting activate appid UTD
```

デバイス上の IOx ベースの TAR ファイルをアクティブにします。

**ステップ 8** **show app-hosting list**

例：

```
Device# show app-hosting list
App id                                   State
---------------------------------------------------------
UTD                                      ACTIVATED

Device#
```

アクティベーションのステータスが表示されます。アプリケーションがアクティブになっていることを確認します。

**ステップ 9** **app-hosting start appid** *name*

例：

```
Device# app-hosting start appid UTD
Device# show app-hosting list | in UTD
```

IOx ベースの OVA を開始します。

**ステップ 10** **show app-hosting list**

例：

```
Example:
Device# show app-hosting list
App id                                   State
---------------------------------------------------------
UTD                                      RUNNING

Device#
```

開始のステータスを表示します。アプリケーションが実行されていることを確認します。

# IOx の設定例

IOx の設定例を次に示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# iox
Device(config)# interface VirtualPortGroup0
Device(config-if)# no shutdown
Device(config-if)# ip address 192.0.2.1 255.255.255.252
Device(config-if)# exit
Device(config)# interface VirtualPortGroup1
Device(config-if)# no shutdown
Device(config-if)# ip address 192.0.2.5 255.255.255.252
Device(config-if)# exit
Device(config)# app-hosting appid utd
Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 0
Device(config-app-hosting-gateway0)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Device(config-app-hosting-gateway0)# exit
Device(config-app-hosting)# app-vnic gateway1 virtualportgroup 1 guest-interface 1
Device(config-app-hosting-gateway1)# guest-ipaddress 192.0.2.6 netmask 255.255.255.252
Device(config-app-hosting-gateway1)# exit
Device(config-app-hosting)# app-resource package-profile custom
Device(config-app-hosting)# start
Device(config-app-hosting)# exit
Device(config)# exit
Device#
```

# Snort IPS のトラブルシューティング

## トラフィックが転送されない

**問題** トラフィックは転送されません。

**考えられる原因** 仮想サービスがアクティブになっていない可能性があります。

**解決法** **show virtual-service list** コマンドを使用して、仮想サービスがアクティブになっているかどうかを確認します。次に、コマンドの出力例を示します。

```
Device# show virtual-service list

Virtual Service List:


Name Status Package Name
------------------------------------------------------------------------------
snort Activated utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
```

**考えられる原因** 指定されたインターフェイスでは、統合脅威防御（UTD）が有効になっていない可能性があります。

**解決法** **show platform software utd global** コマンドを使用して、インターフェイスで UTD が有効になっているかどうかを確認します。

```
Device# show platform software utd global

UTD Global state
Engine               : Standard
Global Inspection    : Disabled
Operational Mode     : Intrusion Prevention
Fail Policy          : Fail-open
Container techonlogy : LXC
Redirect interface   : VirtualPortGroup1
UTD interfaces
GigabitEthernet0/0/0
```

**考えられる原因** サービスノードが正常に動作していない可能性があります。

**解決法** **show platform hardware qfp active feature utd config** コマンドを使用して、サービスノードの状態が緑色かどうかを確認します。

```
Device# show platform hardware qfp active feature utd config

Global configuration
NAT64: disabled
SN threads: 12
CFT inst_id 0 feat id 0 fo id 0 chunk id 4
Context Id: 0, Name: Base Security Ctx
Ctx Flags: (0x60000)
Engine: Standard
SN Redirect Mode : Fail-open, Divert
Threat-inspection: Enabled, Mode: IDS
Domain Filtering : Not Enabled
URL Filtering : Not Enabled
SN Health: Green
```

**考えられる原因** Snort プロセスがアクティブになっていない可能性があります。

**解決法** **show virtual-service detail** コマンドを使用して、Snortプロセス が稼働しているかどうかを確認します。

```
Device# show virtual-service detail

Virtual service UTDIPS detail
  State                  : Activated
  Owner                  : IOSd
  Package information
    Name                 : utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Path                 : bootflash:/utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Application
      Name               : UTD-Snort-Feature
      Installed version  : 1.0.1_SV2982_XE_16_3
      Description        : Unified Threat Defense
    Signing
      Key type           : Cisco development key
      Method             : SHA-1
    Licensing
      Name               : Not Available
      Version            : Not Available
```

```
  Detailed guest status

------------------------------------------------------------------------
Process               Status            Uptime           # of restarts
------------------------------------------------------------------------
climgr                 UP         0Y 0W 0D  0: 0:35        1
logger                 UP         0Y 0W 0D  0: 0: 4        0
snort_1                UP         0Y 0W 0D  0: 0: 4        0
Network stats:
eth0: RX  packets:43, TX  packets:6
eth1: RX  packets:8, TX  packets:6

Coredump file(s): lost+found

  Activated profile name: None
  Resource reservation
    Disk                : 736 MB
    Memory              : 1024 MB
    CPU                 : 25% system CPU

  Attached devices
    Type              Name        Alias
    ---------------------------------------------
    NIC               ieobc_1     ieobc
    NIC               dp_1_0      net2
    NIC               dp_1_1      net3
    NIC               mgmt_1      mgmt
    Disk              _rootfs
    Disk              /opt/var
    Disk              /opt/var/c
    Serial/shell                  serial0
    Serial/aux                    serial1
    Serial/Syslog                 serial2
    Serial/Trace                  serial3
    Watchdog          watchdog-2

  Network interfaces
    MAC address             Attached to interface
    ------------------------------------------------------
    54:0E:00:0B:0C:02       ieobc_1
    A4:4C:11:9E:13:8D       VirtualPortGroup0
    A4:4C:11:9E:13:8C       VirtualPortGroup1
    A4:4C:11:9E:13:8B       mgmt_1

  Guest interface
  ---
  Interface: eth2
  ip address: 48.0.0.2/24
Interface: eth1
  ip address: 47.0.0.2/24

  ---

  Guest routes
  ---
  Address/Mask                      Next Hop                        Intf.
-------------------------------------------------------------------------------
0.0.0.0/0                         48.0.0.1                        eth2
0.0.0.0/0                         47.0.0.1                        eth1

  ---

  Resource admission (without profile) : passed
    Disk space    : 710MB
```

```
Memory         : 1024MB
CPU            : 25% system CPU
VCPUs          : Not specified
```

**考えられる原因** AppNav トンネルがアクティブになっていない可能性があります。

**解決法** **show service-insertion type utd service-node-group** および **show service-insertion type utd service-context** コマンドを使用して、AppNav トンネルがアクティブになっているかどうかを確認します。

**解決法** 次に、**show service-insertion type utd service-node-group** コマンドの出力例を示します。

```
Device# show service-insertion type utd service-node-group

Service Node Group name : utd_sng_1
Service Context : utd/1
Member Service Node count : 1


Service Node (SN) : 30.30.30.2
Auto discovered : No
SN belongs to SNG : utd_sng_1
Current status of SN : Alive
Time current status was reached : Tue Jul 26 11:57:48 2016

Cluster protocol VPATH version : 1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1469514497
Cluster protocol last received sequence number: 1464
Cluster protocol last received ack number : 1469514496
```

**解決法** 次に、**show service-insertion type utd service-context** コマンドの出力例を示します。

```
Device# show service-insertion type utd service-context

Service Context : utd/1
Cluster protocol VPATH version : 1
Time service context was enabled : Tue Jul 26 11:57:47 2016
Current FSM state : Operational
Time FSM entered current state : Tue Jul 26 11:57:58 2016
Last FSM state : Converging
Time FSM entered last state : Tue Jul 26 11:57:47 2016
Cluster operational state : Operational

Stable AppNav controller View:
30.30.30.1

Stable SN View:
30.30.30.2

Current AppNav Controller View:
30.30.30.1

Current SN View:
30.30.30.2
```

**考えられる原因** トラフィックのステータスのデータプレーンUTD統計情報を確認します。トラフィックが転送されない場合、転送および拒否されたパケットの数はゼロになりま

す。数値がゼロ以外の場合、トラフィック転送が行われており、Snort センサーはデータプレーンにパケットを再送信しています。

**解決法** **show platform hardware qfp active feature utd stats** コマンドを使用してトラフィックのステータスを確認します。

```
Device# show platform hardware qfp active feature utd stats

Security Context:    Id:0    Name: Base Security Ctx

Summary Statistics:
Active Connections                                                  29
TCP Connections Created                                         712910
UDP Connections Created                                             80
Pkts entered policy feature                         pkt        3537977
                                                    byt      273232057
Pkts entered divert feature                         pkt        3229148
                                                    byt      249344841
Pkts slow path                                      pkt         712990
                                                    byt       45391747
Pkts Diverted                                       pkt        3224752
                                                    byt      249103697
Pkts Re-injected                                    pkt        3224746
                                                    byt      249103373
….
```

# 署名の更新が機能しない

**問題** Cisco ボーダレスソフトウェア配布（BSD：Borderless Software Distribution）サーバからの署名更新が機能していません。

**考えられる原因** さまざまな理由により署名の更新に失敗した可能性があります。最後に署名の更新に失敗した理由を確認します。

**解決法** **show utd engine standard threat-inspection signature update status** コマンドを使用して、最後に署名の更新に失敗した理由を表示します。

```
Device# show utd eng standard threat-inspection signature update status
Current signature package version: 29.0.c
Current signature package name: default
Previous signature package version: None
----------------------------------------
Last update status: Failed
----------------------------------------
Last successful update time: None
Last successful update method: None
Last successful update server: None
Last successful update speed: None
----------------------------------------
Last failed update time: Thu Jan 11 13:34:36 2018 PST
Last failed update method: Manual
Last failed update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
Last failed update reason: [Errno 113] No route to host
----------------------------------------
Last attempted update time: Thu Jan 11 13:34:36 2018 PST
Last attempted update method: Manual
Last attempted update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
```

```
---------------------------------------
Total num of updates successful: 0
Num of attempts successful: 0
Num of attempts failed: 1
Total num of attempts: 1
---------------------------------------
Next update scheduled at: None
---------------------------------------
Current status: Idle
```

**考えられる原因** ドメインネームシステム（DNS）が正しく設定されていません。

**解決法** **show running-config | i name-server** コマンドを使用して、ネームサーバの詳細を表示します。

```
Device#  show run | i name-server

ip name-server 10.104.49.223
```

**考えられる原因** システムエラー：ユーザ名とパスワードの組み合わせの処理に失敗しました。

**解決法** 署名パッケージのダウンロードに正しい認証情報を使用したことを確認します。

# ローカルサーバからの署名の更新が機能しない

**問題** ローカルサーバからの署名の更新が機能しない。

**考えられる原因** 最後の失敗の理由：無効なスキーム — HTTP または HTTPS のみに対応します。

**解決法** ローカルダウンロード方式として HTTP またはセキュア HTTP（HTTPS）が指定されていることを確認します。

**考えられる原因** 最後の失敗の理由：名前またはサービスが不明です。

**解決法** ローカルサーバに指定されたホスト名または IP アドレスが正しいことを確認します。

**考えられる原因** 最後の失敗の理由：認証情報が入力されていません。

**解決法** ローカル HTTP または HTTPS サーバの認証情報が入力されていることを確認します。

**考えられる原因** 最後の失敗の理由：ファイルが見つかりません。

**解決法** 入力した署名ファイル名または URL が正しいことを確認します。

**考えられる原因** 最後の失敗の理由：ダウンロードが破損しています。

**解決法**

- 以前の署名のダウンロード時に署名更新の再試行でエラーが発生していないかどうかを確認します。
- 正しい署名パッケージが使用可能であることを確認します。

# IOSd Syslog へのロギングが機能しない

**問題** IOSd syslog へのロギングが機能しない。

**考えられる原因** syslog へのロギングは、統合脅威防御（UTD）の設定では設定できません。

**解決法** UTD 設定を表示し、syslog へのロギングが設定されていることを確認するには、**show utd engine standard config** コマンドを使用します。

```
Device# show utd engine standard config

UTD Engine Standard Configutation:
  Operation Mode : Intrusion Prevention
  Policy         : Security

Signature Update:
  Server    : cisco
  User Name : ccouser
  Password  : YEX^SH\fhdOeEGaOBIQAIcOVLgaVGf
  Occurs-at : weekly ;  Days:0 ; Hour: 23; Minute: 50

Logging:
  Server    :   IOS Syslog; 10.104.49.223
  Level     : debug

Whitelist Signature IDs:
  28878
```

**解決法** UTD エンジンのイベントログを表示するには、次の **show utd engine standard logging events** コマンドを使用します。

```
Device# show utd engine standard logging events

2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected]
[Priority: 1] [VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53
2016/06/13-14:32:21.524988 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} a000:0:0:0:0:0:0:10:59964 -> b000:0:0:0:0:0:0:10:53
```

# 外部サーバへのロギングが機能しない

**問題** 外部サーバへのロギングが機能していません。

**考えられる原因** 外部サーバで Syslog が実行されていない可能性があります。

**解決法** syslog サーバが外部サーバで実行されているかどうかを確認します。ステータスを表示するには、外部サーバで次のコマンドを設定します。

```
ps -eaf | grep syslog

 root 2073 1 0 Apr12 ? 00:00:02 syslogd -r -m
```

**考えられる原因** 統合脅威防御（UTD）の Linux コンテナ（LXC：Linux Container）と外部サーバ間の接続が失われている可能性があります。

**解決法** 管理インターフェイスから外部 syslog サーバへの接続を確認します。

## UTD 条件付きデバッグ

条件付きデバッグは、Unified Threat Defense のマルチテナントに対応しています。条件付きデバッグの設定方法の詳細については、以下を参照してください。

http://www.cisco.com/c/en/us/td/docs/routers/asr1000/troubleshooting/guide/Tbl-shooting-xe-3s-asr-1000-book.html#task_AC969BB06B414DCBBDEF7ADD29EF8131

# Snort IPS 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]<br>• 『Cisco IOS Security Command Reference: Commands D to L』[英語]<br>• 『Cisco IOS Security Command Reference: Commands M to R』[英語]<br>• 『Cisco IOS Security Command Reference: Commands S to Z』[英語] |

### 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。<br>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。<br>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 |

# Snort IPS の機能情報

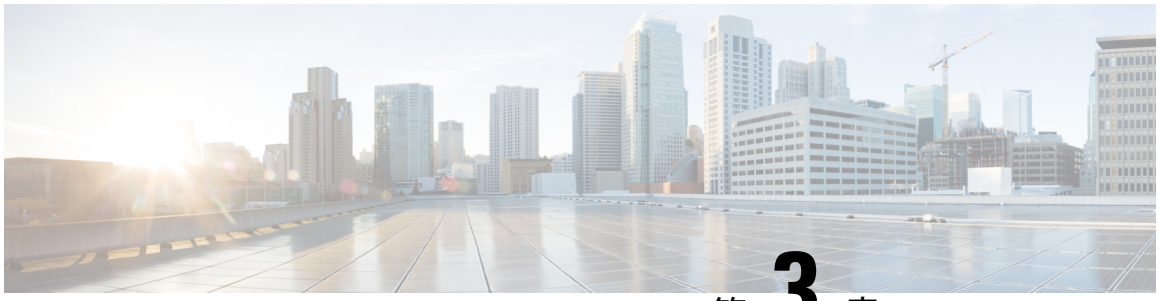
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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 *3 : Snort IPS* の機能情報**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| Snort IPS | Cisco IOS XE 3.16.1S、3.17S 以降のリリース | Snort IPS 機能は、Cisco IOS XE ベースのプラットフォームのブランチオフィスにおける侵入防止システム（IPS：Intrusion Prevention System）および侵入検知システム（IDS）を有効にします。この機能は、オープンソースの Snort ソリューションを使用して IPS と IDS を有効にします。 |
| Snort IPS での VRF 対応 | Cisco IOS XE Denali 16.3.1 | Snort IPS 設定で仮想フラグメンテーションの再構成（VFR：Virtual Fragmentation Reassembl）に対応。 |
| Cisco クラウドサービスルータ 1000v シリーズで Snort IPS に対応 | Cisco IOS XE Denali 16.3.1 | Cisco クラウドサービスルータ 1000v シリーズは Snort IPS に対応します。 |
| 16.4 リリースにおける UTD Snort IPS の機能拡張 | Cisco IOS XE Everest 16.4.1 | 16.4 リリースにおける UTD Snort IPS の機能拡張には、アクティブな署名のリストを表示する機能が追加されています。 |

| 機能名 | リリース | 機能情報 |
|---|---|---|
| 脅威検知アラートの可視性<br><br>UTD サービスの有用性の強化 | Cisco IOS XE Fuji 16.8.1 | この機能は、脅威検知アラートの概要を提供します。次のコマンドが導入されています。<br>• **show utd engine standard logging statistics threat-inspection**<br>• **show utd engine standard logging statistics threat-inspection** *detail*<br><br>次のコマンドは、UTD サービスの有用性の強化の一環として変更されています。<br>• **show utd engine standard status**<br>• **show utd engine standard threat-inspection signature update status** |
| IOX コンテナへの UTD（IPS および URL フィルタリング）の移行 | Cisco IOS XE Gibraltar 16.10.1 | UTD は、仮想サービスコンテナを OVA から IOx に移行することで、Cisco 1100 シリーズ ISR に対応します。 |



第 3 章

# Web フィルタリング

Web フィルタリング機能を使用すると、ドメインベースまたは URL ベースのポリシーとフィルタをデバイスに設定することで、インターネット Web サイトまたはインターネットサイトへのアクセスを制御できます。ユーザは、Web アクセスを管理する Web フィルタリングプロファイルを設定できます。Web フィルタリング機能はコンテナサービスを使用して実装され、これは Snort IPS ソリューションに似ています。

Web フィルタリングでは、以下に基づいて特定のドメインまたは URL へのアクセスを許可または拒否できます。

- 許可リストおよびブロックリスト：これらは静的ルールであり、ユーザがドメインまたは URL を許可または拒否するのに役立ちます。許可リストとブロックリストの両方で同じパターンが設定されている場合、トラフィックは許可されます。
- カテゴリ：URL を、ニュース、ソーシャルメディア、教育、アダルトなどの複数のカテゴリに分類できます。要件に基づいて、ユーザは 1 つ以上のカテゴリをブロックまたは許可することができます。
- レピュテーション：各 URL にはレピュテーションスコアが関連付けられています。レピュテーションスコアの範囲は 0 ー 100 で、高リスク（レピュテーションスコア（0 ー 20）、疑わしい（0 ー 40）、中程度のリスク（0 ー 60）、低リスク（0 ー 80）、信頼できる（0 ー100）に分類されます。URL のレピュテーションスコアと設定に基づいて、URL はブロックまたは許可されます。ユーザが CLI を使用してレピュテーションのしきい値を定義すると、レピュテーションスコアがユーザ定義のしきい値よりも低いすべての URL がブロックされます。

# Web フィルタリング

Web フィルタリング機能を使用すると、ドメインベースまたは URL ベースのポリシーとフィルタをデバイスに設定することで、インターネット Web サイトへのアクセスを制御できます。ドメインベースのフィルタリングでは、ユーザはドメインレベルで Web サイトまたはサーバへのアクセスを制御でき、URL ベースのフィルタリングでは、ユーザは URL レベルで Web サイトへのアクセスを制御できます。この項では、次のトピックについて取り上げます。

## ドメインベースのフィルタリング

ドメインベースのフィルタリングでは、ユーザは、デバイスに設定されたドメインベースのポリシーとフィルタに基づいてアクセスを許可または拒否することで、ドメインへのアクセスを制御できます。クライアントが Cisco クラウドサービスルータ 1000V シリーズを介して DNS 要求を送信すると、DNS トラフィックはドメインベースのポリシー（許可リストまたはブロックリスト）に基づいて検査されます。許可リストまたはブロックリストにあるドメインは、設定されている場合でも URL ベースのフィルタリングの対象になりません。グレーリストのトラフィックは許可リストとブロックリストの両方に一致せず、設定されている場合は URL ベースのフィルタリングの対象となります。

### 許可リストフィルタを使用したドメインベースのフィルタリング

完全なドメイン（cisco.com）をフィルタリングせずに許可するには、許可リストオプションを使用します。ユーザがブラウザを使用して Web サイトにアクセスする要求を行うと、ブラウザは Web サイトの IP アドレスを取得するための DNS 要求を行います。ドメインフィルタリングは、DNS トラフィックにフィルタを適用します。Web サイトのドメイン名が許可リストのパターンのいずれかに一致する場合、ドメインフィルタリングは Web サイトのアドレスを許可リストに追加します。ブラウザが Web サイトの IP アドレスを受信し、Web サイトの IP アドレスに HTTP 要求を送信します。ドメインフィルタリングは、このトラフィックを許可されたトラフィックとして扱います。この許可されたトラフィックは、設定されていても URL ベースのフィルタリングの対象にはなりません。Snort IPS が設定されている場合、トラフィックは Snort IPS の対象となります。

### ブロックリストフィルタを使用したドメインベースのフィルタリング

ユーザがドメイン全体（badsite.com）をブロックする場合は、ブロックリストオプションを使用します。ドメインフィルタリングは、DNS トラフィックにフィルタを適用します。Web サイトのドメイン名がブロックリストのパターンの 1 つと一致する場合、ドメインフィルタリングは、Web サイトの実際に解決された IP アドレスの代わりに、DNS 応答で設定されたブロックサーバの IP アドレスをエンドユーザに送信します。ブラウザは、Web サイトの IP アドレスとしてブロックサーバの IP アドレスを受信し、この IP アドレスに HTTP 要求を送信します。このトラフィックは、設定されている場合でも URL フィルタリングまたは Snort IPS の対象になりません。ブロックサーバは HTTP 要求を受信し、エンドユーザにブロックページを提供します。また、DNS 要求がブロックリストに一致すると、そのドメインへのすべてのアプリケーショントラフィックがブロックされます。

ドメインフィルタリングは、DNS 要求が FTP、Telnet などの非HTTP（S）要求である方法で行われた場合でも、すべての DNS トラフィックに適用されます。ブロックリストに追加されている非HTTP（S）トラフィック（FTP、telnetなど）もブロックサーバに転送されます。ブロックページへの対応または要求の拒否はブロックサーバの役割です。内部または外部ブロックサーバを設定できます。設定手順については、「外部ブロックサーバを使用したドメインベースの Web フィルタリングの設定 （83 ページ）」および「ローカルブロックサーバを使用したドメインベースの Web フィルタリングの設定 （85 ページ）」を参照してください。

ドメインフィルタリング中にトラフィックが許可リストまたはブロックリストに含まれていない場合、URL フィルタリングと Snort IPS が設定されていれば、そのトラフィックは URL フィルタリングと Snort IPS の対象となります。

ユーザは、ドメインフィルタリングの許可パターンリストとブロックパターンリストの組み合わせてフィルタを設計することを検討できます。たとえば、ユーザが許可リスト www\.foo\.com だけでなく、www\.foo\.abc や www\.foo\.xyz などのブロックリストにある他のドメインを作成する場合は、www\.foo\.com を許可リストのパターンに、www\.foo\ をブロックリストのパターンに設定します。

# URL ベースのフィルタリング

URL ベースのフィルタリングにより、ユーザは許可リスト、ブロックリスト、カテゴリ、レピュテーションの設定に基づいて特定の Web サイトへのアクセスを許可または拒否することで、インターネット Web サイトへのアクセスを制御できます。たとえば、クライアントが Cisco CSR 1000V クラウドサービスルータ経由で HTTP 要求を送信すると、HTTP トラフィックは URL フィルタリングポリシー（許可リスト、ブロックリスト、カテゴリ、レピュテーション）に基づいて検査されます。HTTP 要求がブロックリストと一致する場合、HTTP 要求はインラインブロックページ応答によってブロックされるか、URL をブロックサーバにリダイレクトします。HTTP 要求が許可リストと一致する場合、トラフィックはそれ以上の URL フィルタリング検査を行われずに許可されます。

HTTPS トラフィックの場合、インラインブロックページは表示されません。URL ベースのフィルタリングでは、ルックアップを実行する前にエンコードされた URL をデコードしません。

デバイスに許可リストおよびブロックリストの設定がない場合、URL のカテゴリとレピュテーションに基づいて、ブロックページまたは HTTP のリダイレクト URL を使用してトラフィックが許可またはブロックされます。HTTP の場合、ブロックページまたはリダイレクト URL はなく、フローはドロップされます。

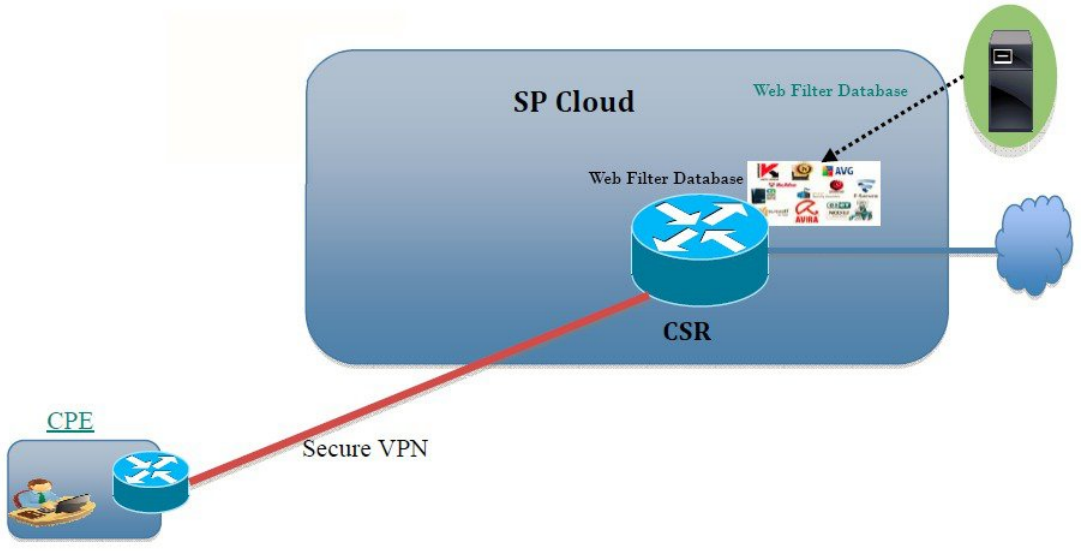
ユーザがカテゴリまたはレピュテーションベースの URL フィルタリングを設定すると、URL データベースがクラウドからダウンロードされます。URL カテゴリまたはレピュテーションデータベースには IP アドレスベースの記録がいくつかあり、カテゴリまたはレピュテーションの検索は、URL のホスト部分にドメイン名がある場合にのみ実行されます。完全なデータベースがクラウドからダウンロードされた後、既存のデータベースに更新がある場合、差分の更新が 15 分ごとに自動的にダウンロードされます。完全なデータベースのサイズは約 440 MB で、ダウンロードしたデータベースは常にクラウドと同期する必要があります。クラウドへの接続が 24 時間以上失われると、データベースは無効になります。

デバイスがクラウドからデータベースの更新を取得しない場合、フェールオープンオプションにより、URL フィルタリング用に指定されたトラフィックがドロップされません。フェールクローズオプションを設定した場合、クラウドの接続が失われると、URL フィルタリング宛てのすべてのトラフィックがドロップされます。

（注） Web フィルタリングデータベースは、15 分ごとにクラウドから定期的に更新されます。

次の図に Web フィルタリングトポロジを示します。

**図 *3 : Web* フィルタリングのネットワークトポロジ**




### URL フィルタリングにおける仮想サービスのリソースプロファイル

Cisco ISR 4000 シリーズサービス統合型ルータは、urlf-low プロファイルとともに urlf-medium および urlf-high リソースプロファイルに対応します。これらのプロファイルは、仮想サービスの実行に必要な CPU およびメモリリソースを表示します。

| プラットフォーム | プロファイル | 仮想サービスのリソース要件 | | プラットフォーム要件 |
|---|---|---|---|---|
| | | システム CPU | SP メモリ | |
| CSR1000v、ISRv | urlf-low | 25% | 3 GB | 8 GB（RAM） |
| | urlf-medium | 50% | 4 GB | 8 GB（RAM） |
| | urlf-high | 75% | 6 GB | 12 GB（RAM） |

# クラウドルックアップ

クラウドルックアップ能は、シングルテナントモードで動作し、ローカルデータベースで使用できない URL のカテゴリとレピュテーションスコアを取得します。クラウドルックアップ機能は、デフォルトで有効になっています。

クラウドルックアップ機能は、オンボックス データベース ルックアップ機能を拡張したものです。以前は、オンボックスデータベースルックアップ機能により、オンボックスデータベースに存在せず、レピュテーションスコアが 0 の URL が許可されていました。クラウドルックアップが有効になっている場合、レピュテーションスコアと設定されたブロックしきい値に基づいて、以前に許可されていた URL がドロップされる場合があります。こういった URL を許可するには、それらの URL をホワイトリストに追加する必要があります。クラウドルックアップのさまざまなURLのカテゴリおよびレピュテーションスコアを以下に説明します。

URL には次の 2 種類があります。

- 名前ベースの URL
- IP ベースの URL

クラウドルックアップ機能を有効にすると、不明な URL のカテゴリとレピュテーションスコアが次のように返されます。

名前ベースの URL

- 有効な URL：対応するカテゴリとレピュテーションスコアが受信されます。
- 不明なURL（新しいURLまたはクラウドに対して未知なURL）：カテゴリは「未分類」、レピュテーションスコアは 40
- 適切なドメイン名を持つ内部URL（例：internal.abc.com）：カテゴリとレピュテーションスコアはベースドメイン名（上記の例の abc.com）に基づきます。
- 完全に内部にある URL（例：abc.xyz）：カテゴリは「未分類」、レピュテーションスコアは 40

IP ベースの URL

- パブリックホスト型 IP：対応するカテゴリとレピュテーションスコアが受信されます。
- プライベート IP（例：10.<>. 192.168.<>）：カテゴリは「未分類」、レピュテーションスコアは 100
- 非ホスト型またはルーティング不可の IP：カテゴリは「未分類」、レピュテーションスコアは 40

クラウドルックアップのスコアは、これらの URL（不明 / 非ホスト型 / ルーティング不可 / 内部 URL）のオンボックスデータベースとは異なります。

（注） クラウドルックアップ機能は、マルチテナントモードでは使用できません。

# Web フィルタリングの利点

Web フィルタリング機能を使用すると、ドメインおよび URL ベースのポリシーとフィルタを設定して、インターネットへのアクセスを制御できます。悪意のあるまたは不要な Web サイトをブロックすることで、ネットワークを保護します。Web フィルタリングは、URL ベースのフィルタリングとドメインベースのフィルタリングで構成されています。ドメインベースのフィルタリングは、ドメインレベルで Web サイトまたはサーバへのアクセスを制御し、URL ベースのフィルタリングは、URL レベルで Web サイトへのアクセスを制御します。ユーザは Web フィルタリングを使用して、個別の URL をブロックリストまたはドメイン名に追加し、その同じ URL に対して許可リストのポリシーを設定できます。ユーザは、レピュテーションまたはカテゴリに基づいて URL を許可またはブロックするようにプロビジョニングすることもできます。

# Web フィルタリングの前提条件

Cisco CSR 1000V クラウドサービスルータで Web フィルタリング機能を設定する前に、次のことを確認します。

- Cisco CSR 1000V クラウドサービスルータは、Cisco IOS XE Denali 16.3 以降のソフトウェアイメージを実行します。
- Cisco CSR 1000V クラウドサービスルータには、コンテナサービスを導入するために 2 つの vCPU、8 GB のメモリ、および 2 GB の追加のディスク領域が必要となります。
- Cisco CSR 1000V クラウドサービスルータには、Web フィルタリング機能を有効にするためのセキュリティ K9 ライセンスが必要です。

# Web フィルタリングの制約事項

Web フィルタリング機能には、次のような制約事項が適用されます。

- この機能は、Cisco CSR 1000V クラウドサービスルータのみに対応し、Cisco 4000 シリーズサービス統合型ルータには対応しません。
- 許可リストおよびブロックリストのパターンは正規表現のパターンのみに対応し、現在は許可リストおよびブロックリストでは 64 個のパターンに対応しています。正規表現のパターンの詳細については、「正規表現」の章を参照してください。
- ドメインフィルタリングは、IPv4 UDP 転送を使用して DNS プロトコルで解決された IPv4 ドメインのみに対応します。ドメイン フィルタリング アラートは、IOS syslog にのみ送信されます。
- OpenDNS によるドメインフィルタリングには対応していません。

- 仮想ルーティングおよび転送（VRF：Virtual Routing and Forwarding）を使用した URL フィルタリングには対応していません。
- CWS によるドメインフィルタリングには対応していません。
- ドメインフィルタリングは、カテゴリとレピュテーションに対応していません。
- ローカルブロックサーバは、HTTPS ブロックページの提供には対応していません。URL フィルタがブロックページまたはリダイレクトメッセージを挿入しようとする場合、HTTPS トラフィックには対応しません。
- URL にユーザ名とパスワードがある場合、URL フィルタは許可リストおよびブロックリストのパターンと一致させる前に URL からそれらを削除することはしません。ただし、カテゴリまたはレピュテーションルックアップにはこの制限はなく、ルックアップの前に URL からユーザ名とパスワードを削除します。
- HTTPS 検査は制限されています。Web フィルタリングでは、サーバ証明書を使用して URL およびドメイン情報を取得します。完全な URL のパスを検査することはできません。
- UTD は、VRF 間シナリオにおいては WCCP および NBAR との相互運用は行いません。
- URL、ドメイン、ブロック、sourcedb の Web フィルタのプロファイル名に使用できるのは、英数字、ダッシュ、および下線のみです。
- 仮想サービスプロファイルが変更された場合、プロファイルの変更を有効にするには、仮想サービスを再インストールする必要があります。

# Web フィルタリングの導入方法

対応しているデバイスに Web フィルタリングを導入するには、次のタスクを実行します。

### 始める前に

- **デバイスのプロビジョニング**：Web フィルタリング機能をインストールするデバイスを特定します。この機能は、Cisco CSR 1000V クラウドサービスルータに対応しています。
- **ライセンスの取得**：Web フィルタリング機能は、サービスを有効にするためにセキュリティライセンスが必要なセキュリティパッケージでのみ使用できます。ライセンスの取得については、シスコ サポートにお問い合わせください。

**ステップ 1** 仮想コンテナサービスをインストールしてアクティブにします。仮想コンテナサービスのインストールおよびアクティブ化の方法 （82 ページ）

**ステップ 2** 外部ブロックサーバを使用してドメインベースの Web フィルタリングを設定します。外部ブロックサーバを使用したドメインベースの Web フィルタリングの設定 （83 ページ）

**ステップ 3** ローカルブロックサーバを使用してドメインベースの Web フィルタリングを設定します。ローカルブロックサーバを使用したドメインベースの Web フィルタリングの設定 （85 ページ）

**ステップ 4** ローカルブロックサーバを使用して URL ベースの Web フィルタリングを設定します。ローカルブロックサーバを使用した URL ベースの Web フィルタリングの設定 （86 ページ）

**ステップ 5** インラインブロックサーバを使用して URL ベースの Web フィルタリングを設定します。インラインブロックページを使用した URL ベースの Web フィルタリングの設定 （88 ページ）

**ステップ 6** Snort IPS または IDSを設定します。ドメインおよび URL ベースの Web フィルタリングと Snort IPS の設定（90 ページ）

# 仮想コンテナサービスのインストールおよびアクティブ化の方法

仮想コンテナサービスをインストールしてアクティブにするには、次のタスクを実行します。

**ステップ 1** UTD OVA ファイルをインストールします。UTD OVA ファイルのインストール （82 ページ）

**ステップ 2** VirtualPortGroup のインターフェイスおよび仮想サービスを設定します。VirtualPortGroup のインターフェイスおよび仮想サービスの設定 （82 ページ）

**ステップ 3** Snort 仮想コンテナサービスをアクティブにします。

# UTD OVA ファイルのインストール

OVA ファイルは、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。この OVA ファイルをルータにダウンロードし、仮想サービスのインストール CLI を使用してサービスをインストールする必要があります。サービス OVA ファイルは、ルータにインストールされている Cisco IOS XE リリースイメージには付属していません。ただし、OVA ファイルはルータのフラッシュに事前にインストールされている場合があります。

セキュリティライセンスが付属した Cisco IOS XE イメージを使用する必要があります。OVA ファイルのインストール中に、セキュリティライセンスがチェックされ、ライセンスが存在しない場合はエラーが報告されます。

これはサンプル設定です。

```
Device> enable
Device# virtual-service install name UTDIPS package harddisk:utd-ips-v102.ova media
harddisk:
Device# show virtual-service list
Virtual Service List:
Name Status Package Name
------------------------------------------------------------------------------
snort Installed utdsnort.1_2_2_SV2982_XE_main.20160
```

# VirtualPortGroup のインターフェイスおよび仮想サービスの設定

2 つの VirtualPortGroup インターフェイスと両方のインターフェイスのゲスト IP アドレスを設定する必要があります。

（注） データトラフィック用の VirtualPortGroup インターフェイスは、プライベートまたはルーティング不可の IP アドレスを使用する必要があります。このインターフェイスには、IP アドレスの範囲として 192.0.2.0 / 30を 使用することを推奨します。

これはサンプル設定です。

```
Device# configure terminal
evice(config)# interface VirtualPortGroup0
Device(config-if)# ip address 192.0.2.1 255.255.255.252
Device(config-if)# exit
Device(config)# interface VirtualPortGroup 1
Device(config-if)# ip address 192.0.2.5 255.255.255.252
Device(config-if)# exit
Device(config)# virtual-service UTDIPS

Device(config-virt-serv)# profile urlf-low (This is minimum requirement for web filtering
 to work.)

Device(config-virt-serv)# vnic gateway VirtualPortGroup 0 (The IP-address configured in
 VPG0 interface should have access to Internet over http(s).If the VPG0 interface does
not have access to Internet, the web filter database will not be updated.)
Device(config-virt-serv-vnic)# guest ip address 192.0.2.2
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# vnic gateway VirtualPortGroup 1
Device(config-virt-serv-vnic)# guest ip address 192.0.2.6
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# activate
Device(config-virt-serv)# end

Device# show virtual-service list
Virtual Service List:

Name                      Status              Package Name
------------------------------------------------------------------------------
snort                     Activated           utdsnort.1_2_2_SV2982_XE_main.20160
```

# 外部ブロックサーバを使用したドメインベースのWebフィルタリングの設定

外部ブロックサーバを使用してドメインベースの Web フィルタリングを設定するには、次の手順を実行します。

**ステップ 1** 仮想サービスをインストールし、アクティブにします。詳細については、VirtualPortGroup のインターフェイスおよび仮想サービスの設定 （82 ページ）を参照してください。

**ステップ 2** ブロックリストのパラメータマップを次のように設定します。

```
parameter-map type regex domainfilter_blacklist_pmap1
  pattern examplebook\.com
  pattern bitter\.com
```

**ステップ 3** 許可リストのパラメータマップを次のように設定します。

```
parameter-map type regex domainfilter_whitelist_pmap1
  pattern example\.com
  pattern exmaplegogle\.com
```

**ステップ 4** ドメインプロファイルを設定し、ブロックリストと許可リストのパラメータマップを次のように関連付けます。

```
utd web-filter domain profile 1
 blacklist
  parameter-map regex domainfilter_blacklist_pmap1
 whitelist
  parameter-map regex domainfilter_whitelist_pmap1
```

**ステップ 5** （オプション）デフォルトでは、ドメインフィルタリングアラートは有効になっていません。ドメインプロファイルでブロックリストまたは許可リスト、あるいはその両方のアラートを設定します。

```
alert {all | blacklist | whitelist}
```

**ステップ 6** ドメインプロファイルで外部リダイレクトサーバを設定します。

```
redirect-server external x.x.x.x (This is the IP address that is used for serving block page when
a page is on the blocked list)
```

**ステップ 7** 次のドメインプロファイルを使用して UTD エンジン標準を設定します。

```
utd engine standard
 web-filter
  domain-profile 1
```

**ステップ 8** エンジン標準を使用してUTDを設定し、グローバルに、または特定のインターフェイスで有効にします。

```
utd
  all-interfaces
  engine standard
```

次に、外部ブロックサーバを使用してドメインベースの Web フィルタリングを設定する例を示します。

```
parameter-map type regex domainfilter_blacklist_pmap1
  pattern examplebook\.com
  pattern bitter\.com
parameter-map type regex domainfilter_whitelist_pmap1
  pattern exmaplegogle\.com
  pattern exmaplegogle\.com
utd engine standard
  web-filter
    domain-profile 1
!
utd web-filter domain profile 1
  alert all
  blacklist
    parameter-map regex domainfilter_blacklist_pmap1
  whitelist
    parameter-map regex domainfilter_whitelist_pmap1
  redirect-server external 192.168.1.1
!
utd
  all-interfaces
  engine standard
```

# ローカルブロックサーバを使用したドメインベースのWebフィルタリングの設定

ローカルブロックサーバでを使用してドメインベースの Web フィルタリングを設定するには、次の手順を実行します。

**ステップ 1** 仮想サービスをインストールし、アクティブにします。詳細については、VirtualPortGroup のインターフェイスおよび仮想サービスの設定 （82 ページ）を参照してください。

**ステップ 2** ループバックインターフェイスを設定するか、クライアントがアクセスできる既存のインターフェイスを使用します。

```
interface loopback 110
 ip address 10.1.1.1 255.255.255.255
exit
```

**ステップ 3** ローカルブロックサーバのプロファイルを使用して UTD Web フィルタを設定します。

```
utd web-filter block local-server profile 1
 block-page-interface loopback 110
 http-ports 80
 content text "Blocked by Web-Filter"
```

**ステップ 4** ブロックリストのパラメータマップを次のように設定します。

```
parameter-map type regex domainfilter_blacklist_pmap1
  pattern bitter\.com
```

**ステップ 5** 許可リストのパラメータマップを次のように設定します。

```
parameter-map type regex domainfilter_whitelist_pmap1
  pattern sweet\.com
```

**ステップ 6** ドメインプロファイルを設定し、ブロックリストと許可リストのパラメータマップを次のように関連付けます。

```
utd web-filter domain profile1
 blacklist
  parameter-map regex domainfilter_blacklist_pmap1
 whitelist
  parameter-map regex domainfilter_whitelist_pmap1
```

**ステップ 7** （オプション）デフォルトでは、ドメインフィルタリングアラートは有効になっていません。ドメインプロファイルでブロックリストまたは許可リスト、あるいはその両方のアラートを設定します。

```
alert {all |blacklist | whitelist}
```

**ステップ 8** ドメインプロファイルでリダイレクトサーバをローカルブロックサーバとして設定します。

```
redirect-server local-block-server 1
```

**ステップ 9** 次のドメインプロファイルを使用して UTD エンジン標準を設定します。

```
utd engine standard
 web-filter
  domain-profile 1
```

**ステップ 10** エンジン標準を使用して UTD を設定し、グローバルに、または特定のインターフェイスで有効にします。

```
utd
  all-interfaces
  engine standard
```

次に、ローカルブロックサーバを使用してドメインベースの Web フィルタリングを設定する例を示します。

```
interface loopback 110
  ip address 10.1.1.1 255.255.255.255
exit
parameter-map type regex domainfilter_blacklist_pmap1
  pattern bitter\.com
parameter-map type regex domainfilter_whitelist_pmap1
  pattern sweet\.com
utd engine standard
  web-filter
    domain-profile 1
!
utd web-filter block local-server profile 1
  block-page-interface Loopback110
  content text "Blocked by Web-Filter"
  http-ports 80
!
utd web-filter domain profile 1
  alert all
  blacklist
    parameter-map regex domainfilter_blacklist_pmap1
  whitelist
    parameter-map regex df_whitelist_pmap1
  redirect-server local-block-server 1
!
utd
  all-interfaces
  engine standard
```

# ローカルブロックサーバを使用した URL ベースの Web フィルタリングの設定

ローカルブロックサーバを使用して URL ベースの Web フィルタリングを設定するには、次の手順を実行します。

**ステップ 1** 仮想サービスをインストールし、アクティブにします。詳細については、VirtualPortGroup のインターフェイスおよび仮想サービスの設定 （82 ページ）を参照してください。

**ステップ 2** ループバックインターフェイスを設定するか、クライアントがアクセスできる既存のインターフェイスを使用します。

```
interface loopback 110
 ip address 10.1.1.1 255.255.255.255
exit
```

**ステップ 3** ローカルブロックサーバのプロファイルを使用して UTD Web フィルタを設定します。

```
utd web-filter block local-server profile 1
 block-page-interface loopback 110
 http-ports 80
 content text "Blocked by Web-Filter"
```

**ステップ 4** ブロックリストのパラメータマップを次のように設定します。

```
parameter-map type regex urlf_blacklist_pmap1
 pattern exmplee.com/sports
```

**ステップ 5** 許可リストのパラメータマップを次のように設定します。

```
parameter-map type regex urlf_whitelist_pmap1
 pattern examplehoo.com/finance
```

**ステップ 6** URL プロファイルを設定し、次の手順を実行します。

```
utd web-filter url profile 1
```

a) ブロックリストと許可リストのパラメータマップを関連付けます。

```
blacklist
  parameter-map regex urlf_blacklist_pmap1
whitelist
  parameter-map regex urlf_whitelist_pmap1
```

b) ローカルブロックサーバのプロファイルでブロックリスト、許可リスト、またはその両方のアラートを設定します。

```
alert {all | blacklist | whitelist}
```

c) 許可またはブロックするカテゴリを設定します。

```
categories allow
  sports
```

d) レピュテーションブロックのしきい値を設定します。

```
reputation
  block-threshold high-risk
```

e) フェールオプションを使用して URL ソースデータベースを設定します。

```
sourcedb fail close
```

f) ログレベルを設定します。デフォルトオプションはエラーです。オプションを [info] または [detail] に設定すると、パフォーマンスが次の影響を受ける可能性があります。

```
log level error
```

g) ローカルブロックサーバをブロックに設定します。

```
block local-server 1
```

**ステップ 7** URL プロファイルを使用して UTD エンジン標準を設定します。

```
utd engine standard
 web-filter
   url-profile 1
```

**ステップ 8** UTD エンジン標準を設定し、グローバルまたは特定のインターフェイスで UTD を有効にします。

```
utd
  all-interfaces
  engine standard
```

次に、ローカルブロックサーバを使用して URL ベースの Web フィルタリングを設定する例を示します。

```
parameter-map type regex urlf_blacklist_pmap1
 pattern examplee.com/sports
parameter-map type regex urlf_whitelist_pmap1
 pattern exmaplehoo.com/finance
!
interface loopback 110
 ip address 10.1.1.1 255.255.255.255
 exit
utd web-filter block local-server profile 1
 block-page-interface loopback 110
 http-ports 80
 content text "Blocked by Web-Filter"
utd web-filter url profile 1
 blacklist
  parameter-map regex urlf_blacklist_pmap1
 whitelist
  parameter-map regex urlf_whitelist_pmap1
 alert all
 categories allow
  sports
 reputation
  block-threshold high-risk
 sourcedb fail close
 log level error
 block local-server 1
!
utd engine standard
 web-filter
  url-profile 1
!
utd
 all-interfaces
 engine standard
```

# インラインブロックページを使用した URL ベースの Web フィルタリングの設定

インラインブロックページを使用して URL ベースの Web フィルタリングを設定するには、次の手順を実行します。

**ステップ 1** 仮想サービスをインストールし、アクティブにします。詳細については、VirtualPortGroup のインターフェイスおよび仮想サービスの設定 （82 ページ）を参照してください。

**ステップ 2** ブロックリストのパラメータマップを次のように設定します。

```
parameter-map type regex urlf_blacklist_pmap1
 pattern exmaplegogle.com/sports
```

**ステップ 3** 許可リストのパラメータマップを次のように設定します。

```
parameter-map type regex urlf_whitelist_pmap1
 pattern exmaplehoo.com/finance
```

**ステップ 4** UTD ブロックページのプロファイルを設定します。

```
utd web-filter block page profile 1
 text "Blocked by Web-Filter URLF" (The other options are file and redirect-url)
```

**ステップ 5** URL プロファイルを設定し、次の手順を実行します。

```
utd web-filter url profile 1
```

a) ブロックリストと許可リストのパラメータマップを関連付けます。

```
blacklist
  parameter-map regex urlf_blacklist_pmap1
whitelist
  parameter-map regex urlf_whitelist_pmap1
```

b) ローカルブロックサーバのプロファイルでブロックリスト、許可リスト、またはその両方のアラートを設定します。

```
alert {all | blacklist | whitelist | categories-reputation}
```

c) 許可またはブロックするカテゴリを設定します。

```
categories allow
  sports
```

d) レピュテーションブロックのしきい値を設定します。

```
reputation
  block-threshold high-risk
```

e) フェールオプションを使用して URL ソースデータベースを設定します。

```
sourcedb fail close
```

f) ログレベルを設定します。デフォルトオプションはエラーです。オプションを [info] または [detail] に設定すると、パフォーマンスが次の影響を受ける可能性があります。

```
log level error
```

g) ローカルブロックサーバをブロックに設定します。

```
block local-server 1
```

**ステップ 6** URL プロファイルを使用して UTD エンジン標準を設定します。

```
utd engine standard
 web-filter
   url-profile 1
```

**ステップ 7** UTD エンジン標準を設定し、グローバルまたは特定のインターフェイスで UTD を有効にします。

```
utd
  all-interfaces
  engine standard
```

次に、インラインブロックサーバを使用してURLベースのWebフィルタリングを設定する例を示します。

```
parameter-map type regex urlf_blacklist_pmap1
  pattern exmaplegogle.com/sports
parameter-map type regex urlf_whitelist_pmap1
 pattern exmaplehoo.com/finance
!
utd web-filter block page profile 1
 text "Blocked by Web-Filter URLF"
!
utd web-filter url profile 1
 blacklist
  parameter-map regex urlf_blacklist_pmap1
 whitelist
  parameter-map regex urlf_whitelist_pmap1
 alert all
 categories allow
  sports
 reputation
  block-threshold high-risk
 sourcedb fail close
 log level error
!
utd engine standard
 web-filter
  url-profile 1
!
utd
 all-interfaces
 engine standard
```

# ドメインおよび URL ベースの Web フィルタリングと Snort IPS の設定

ドメインまたはURLベースのWebフィルタリングとSnort IPSを設定するには、次の手順を実行します。

**ステップ 1** ドメインプロファイルを設定します。

```
utd web-filter domain profile 1
```

**ステップ 2** URL プロファイルを設定します。

```
utd web-filter url profile 1
```

**ステップ 3** UTD エンジン標準で脅威検知を設定します。

```
utd engine standard
 threat-inspection
```

**ステップ 4** ドメインプロファイルと URL プロファイルを使用して、UTD エンジン標準で Web フィルタを設定します。

```
utd engine standard
 logging syslog
 threat-inspection
  threat protection
```

```
 policy security
signature update server cisco username xxx password QhLb]Z[ifMbFgLYgR]^KLDUZ
 signature update occur-at daily 0 0
 logging level error
web-filter
 domain-profile 1
 url-profile 1
```

**ステップ 5** UTD エンジン標準を設定し、グローバルに、または特定のインターフェイスで有効にします。

```
utd
  all-interfaces
  engine standard
```

# Web フィルタ設定の確認

次のコマンドを使用して、Web フィルタリングの設定を確認できます。

```
Device# show utd engine standard config

UTD Engine Standard Configuration:
  Operation Mode : Intrusion Detection
  Policy         : Balanced

  Signature Update: Not Configured

  Logging:
    Server    :  IOS Syslog
    Level     : err (Default)
    Statistics    : Disabled

  Whitelist : Disabled
  Whitelist Signature IDs:

Web-Filter      : Enabled

  Whitelist :
    www.cisco.com
  Blacklist :
    www.hotstar.com

  Categories Action : Block
  Categories :
    Fashion and Beauty

  Block Profile:
   No config present

  Reputation Block Threshold : Moderate risk
  Alerts Enabled : Blacklist
  Cloud Lookup : Enabled
  Debug level : Error
Conditional debug level : Error
```

# Web フィルタリングのトラブルシューティング

ログを収集するには、**virtual-service move name "CONTAINER_NAME" log to bootflash:** コマンドを使用します。デバイスで次のコマンドを使用して、Web フィルタリング機能の有効化に関連する問題のトラブルシューティングを行うことができます。

- **debug utd engine standard all**
- **debug utd engine standard climgr**
- **debug utd engine standard daq**
- **debug utd engine standard internal**
- **debug utd engine standard onep**

リリース 16.8.1 では、コンテナの設定および署名の更新を適用するために、コンテナの設定エラーの回復が強化されています。強化されたエラー修復により、次のことが可能になります。

- エラーを検出して対処するための、設定をダウンロードする際の安定性の向上。
- 署名と設定の更新を同時に処理する効率的な方法。
- IOSd と CLIMGR 間の oneP 接続が失われた際の早期における検出と回復。たとえば、CLIMGR がクラッシュした場合など。
- （現在または最近の）設定ダウンロードの詳細結果の可視性の向上（デバッグを有効にする必要はありません）。

# 設定例

次に、CSR 1000V クラウドサービスルータでドメインフィルタリングを有効にする例を示します。

```
Device# configure terminal
Device(config)# parameter-map type regex wlist1
Device(config-profile)# pattern google.com
Device(config-profile)# pattern cisco.com
Device(config-profile)# exit
Device(config)# parameter-map type regex blist1
Device(config-profile)# pattern exmaplehoo.com
Device(config-profile)# pattern bing.com
Device(config-profile)# exit
Device(config)# utd web-filter block local-server profile 1
Device(config--utd-webf-blk-srvr)# content file bootflash:test.utd.file
Device(config--utd-webf-blk-srvr)# end
```

ローカルブロックサーバを動作させるには、HTTP サーバが稼働している必要があります。ip http server コマンドを使用して、ブロックサーバを設定します。show ip http server status コマンドは、サーバのステータスを有効として表示します。

```
Device# show ip http server status
HTTP server status: Enabled
HTTP server port: 80
```

# 例：Web フィルタのドメインプロファイルの設定

次の例は、Web フィルタのドメインプロファイルを設定する方法を示しています。

```
Device(config)# utd web-filter domain profile 1
Device(config-utd-webfltr-domain)# blacklist
Device(config-utd-webf-dmn-bl)# parameter-map regex blist1
Device(config-utd-webf-dmn-bl)# whitelist
Device(config-utd-webf-dmn-wl)# parameter-map regex wlist1
Device(config-utd-webf-dmn-wl)# exit
Device(config-utd-webfltr-domain)# alert all
Device(config-utd-webfltr-domain)# redirect-server external 1.2.3.4
Device(config-utd-webfltr-domain)# exit
```

# Web フィルタの URL プロファイルの設定

次の例は、Web フィルタの URL プロファイルを設定する方法を示しています。

```
Device(config)# utd web-filter url profile 1
Device(config-utd-webfltr-url)# blacklist
Device(config-utd-webf-url-bl)# parameter-map regex blist1
Device(config-utd-webf-url-bl)# whitelist
Device(config-utd-webf-url-wl)# parameter-map regex wlist1
Device(config-utd-webf-url-wl)# exit
Device(config-utd-webfltr-url)# categories allow
Device(config-utd-webf-url-cat)# news-and-media
Device(config-utd-webf-url-cat)# search-engines
Device(config-utd-webf-url-cat)# computer-and-internet-info
Device(config-utd-webf-url-cat)# computer-and-internet-security
Device(config-utd-webf-url-cat)# financial-services
Device(config-utd-webf-url-cat)# image-and-video-search
Device(config-utd-webf-url-cat)# job-search
Device(config-utd-webf-url-cat)#exit
Device(config-utd-webfltr-url)# alert all
Device(config-utd-webfltr-url)# reputation
Device(config-utd-webf-url-rep)# block-threshold suspicious
Device(config-utd-webf-url-rep)# exit
Device(config-utd-webfltr-url)# block local-server 1
Device(config-utd-webfltr-url)# exit
```

# UTD Snort IPS または IDS のホワイトリスト署名の設定

次の例は、署名のホワイトリストを設定する方法を示しています。

```
Device(config)# utd threat-inspection whitelist
Device(config-utd-whitelist)# generator id 1 signature id 1
Device(config-utd-whitelist)# generator id 1 signature id 2
Device(config-utd-whitelist)# exit
```

# 例：Web フィルタプロファイルの設定

次の例は、Web フィルタのプロファイルを設定する方法を示しています。

```
Device(config)# utd engine standard
Device(config-utd-eng-std)# logging server 1.2.3.4
Device(config-utd-eng-std)# threat-inspection
```

```
Device(config-utd-engstd-insp)#threat protection
Device(config-utd-engstd-insp)# policy security
Device(config-utd-engstd-insp)# logging level emerg
Device(config-utd-engstd-insp)# whitelist
Device(config-utd-engstd-insp)# web-filter
Device(config-utd-engstd-webf)# domain-profile 1
Device(config-utd-engstd-webf)# url-profile 1
Device(config-utd-engstd-webf)# exit
```

# 例：Web フィルタリングイベントのアラートメッセージ

次に、Web フィルタリングイベントのアラートメッセージの例を示します。

```
016/06/02-14:44:41.061501 IST [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Blacklist
 [**] [URL: www.edition.cnn.com/2016/03/31/asia/kolkata-bridge-collapse/index.html]
[Initiator_VRF: 0] {TCP} 1.0.0.9:56608 -> 2.0.0.29:80

2016/06/02-14:48:06.636270 IST [**] [Instance_ID: 1] [**] Pass [**] UTD WebFilter Whitelist
 [**] [URL: www.ndtv.com/index.html] [Initiator_VRF: 0] {TCP} 1.0.0.9:56611 -> 2.0.0.23:80

Jun 2 14:37:57.856 IST: %IOSXE-6-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:000
TS:00000618422205723793 %UTD-6-UTD_DF_BLACKLIST_MATCH: UTD WebFilter Domain Blacklist
[**] [Domain: www.cricinfo.com] [Matched Pattern: www.cricinfo.com] {UDP} 2.0.0.10:53
-> 1.0.0.9:55184

Jun 2 14:39:22.653 IST: %IOSXE-6-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:000
TS:00000618507002407540 %UTD-6-UTD_DF_WHITELIST_MATCH: UTD WebFilter Domain Whitelist
[**] [Domain: www.cricinfo.com] [Matched Pattern: www.cricinfo.com] {UDP} 2.0.0.10:53
-> 1.0.0.9:55286
```

# 例：クラウドルックアップの設定解除

次に、Web フィルタリングでクラウドルックアップ機能を設定解除する例を示します。

```
Device(config)# utd engine standard
Device(config-utd-eng-std)# web-filter
% Please ensure urlf-<low/medium/high> virtual-service profile is configured to use the
 web-filter feature

Device(config-utd-engstd-webf)# no cloud-lookup
Device(config-utd-engstd-webf)# end
Device # exit
```

# Cisco Web フィルタリングに関する追加の参考資料

**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] |

| 関連項目 | マニュアル タイトル |
|---|---|
| セキュリティ コマンド | • 『Cisco IOS Security Command Reference: Commands A to C』[英語]<br>• 『Cisco IOS Security Command Reference: Commands D to L』[英語]<br>• 『Cisco IOS Security Command Reference: Commands M to R』[英語]<br>• 『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。<br>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。<br>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 |

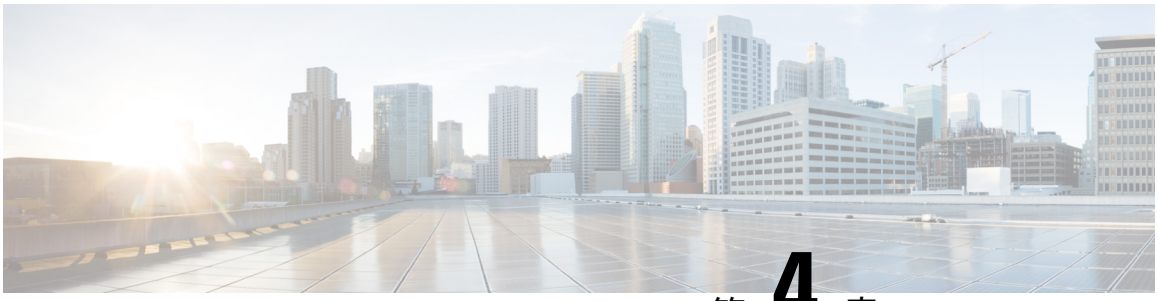
# Cisco Web フィルタリングに関する機能情報

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 *4 : Cisco Web* フィルタリングに関する機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| Cisco Web フィルタリング | Cisco IOS XE Denali リリース 16.3.1 | Web フィルタリング機能を使用すると、ドメインベースまたは URL ベースのポリシーとフィルタをデバイスに設定することで、インターネット Web サイトへのアクセスを制御できます。ユーザは Web フィルタリングのプロファイルを設定して Web アクセスを管理できます。Web フィルタリング機能はコンテナサービスを使用して実装され、これは Snort IPS ソリューションに似ています。 |
| ISRv の UTD 機能パリティ<br>UTD サービスの有用性の強化 | Cisco IOS XE Fuji リリース 16.8.1 | CSR では、シングルテナントモードとマルチテナントモードの両方でのドメインおよび URL フィルタリングに対応しています。ISRv では、シングルテナントのみに対応しています。この機能は、ENCS プラットフォームのすべてのモデルで使用できます。<br>UTD のエラー回復機能が強化され、IOS から一括設定のダウンロードを開始することで、コンテナが内部エラーから回復できるようになりました。<br>コマンド **utd web-filter** *profile name* が変更されています。 |
| Web ルート URL フィルタリングの機能強化 | Cisco IOS XE Fuji リリース 16.9.1 | Web フィルタリングの URLF 仮想リソースプロファイルは、プラットフォーム CSR1000v および ISRv にのみ対応します。<br>URL フィルタリングは、データベースに存在しないクラウド内の URL を検索するクラウドルックアップ機能に対応しています。 |



第 4 章

# 統合脅威防御（UTD）のマルチテナントの設定

統合脅威防御（UTD）のマルチテナントは、複数のユーザに Snort IPS と Web フィルタリングを提供します。1 つの Cisco CSR 1000v インスタンスで 1 つ以上のテナントのポリシーを定義できます。各ポリシーには、脅威検知プロファイルと Web フィルタリングプロファイルを設定できます。次の項では、Unified Threat Defense のマルチテナントを設定する方法について説明します。これらの設定手順で使用されるコマンドの多くは、シングルテナントの設定で使用されるものと似ています。Snort IPS （23 ページ） および Web フィルタリング （75 ページ） を参照してください。



## 統合脅威防御（UTD）のマルチテナントに関する情報

Snort IPS および Web フィルタリングのマルチテナントを使用すると、1 つの Cisco CSR 1000v のインスタンスで 1 つ以上のテナントのポリシーを定義できます。この機能は、Cisco IOS XE Everest 16.6.1 で導入されました。

各テナントは、1 つ以上の VPN ルーティングおよび転送テーブル（VRF）を持つ VPN ルーティングおよび転送インスタンスです。統合脅威防御（UTD）のポリシーは、脅威検知プロファイルと Web フィルタリングプロファイルに関連付けられています。複数のテナントが UTD ポリシーを共有できます。

システムログには、テナントごとの統計情報を生成を可能にする VRF の名前が含まれます。

マルチテナントモードで使用する CLI コマンドは、シングルテナントモードで使用するものと似ています（Snort IPS （23 ページ） および Web フィルタリング （75 ページ） を参照）。

マルチテナントでは、サブモードである `utd engine standard multi-tenancy`に入り、UTD ポリシー、Web フィルタリング、および脅威検知プロファイルを設定します。`utd engine standard multi-tenancy`のサブモードを終了すると、UTD ポリシーが適用されます。

Web フィルタリングと脅威検知（Snort IPS または IDS）の利点については、次の項で説明します。

- Web フィルタリングの利点
- Snort IPS の概要
- Snort IPS ソリューション
- Snort 仮想サービスインターフェイスの概要

# Web フィルタリングの概要

Web フィルタリングにより、URL ベースのポリシーとフィルタを設定することで、インターネットへのアクセスを制御できます。Web フィルタリングは、悪意のあるもしくは不要な Web サイトをブロックし、ネットワークのセキュリティを強化することで、Web サイトへのアクセスの制御に役立ちます。個々の URL またはドメイン名をブロックリストに載せ、それらに対して許可リストポリシーを設定できます。レピュテーションまたはカテゴリに基づいて URL を許可またはブロックするようにプロビジョニングすることもできます。

# Snort IPS の概要

Snort IPS 機能は、Cisco 4000 シリーズサービス統合型ルータおよび Cisco クラウドサービスルータ 1000v シリーズのブランチオフィスで侵入防止システム（IPS）または侵入検知システム（IDS）を実現します。この機能は、Snort エンジンを使用して IPS および IDS 機能を実現します。

Snort は、リアルタイムでトラフィック分析を行い、IP ネットワークで脅威が検出されたときにアラートを生成するオープンソースのネットワーク IPS です。また、プロトコル分析、コンテンツ検索またはマッチングを実行し、バッファオーバーフロー、ステルスポートスキャンなどのさまざまな攻撃やプローブを検出することもできます。Snort エンジンは、Cisco 4000 シリーズサービス統合型ルータおよび Cisco クラウドサービスルータ 1000v シリーズで仮想コンテナサービスとして実行されます。

Snort IPS 機能は、IPS または IDS 機能を提供するネットワーク侵入検知および防止モードで動作します。ネットワーク侵入検知および防止モードでは、Snort は次のアクションを実行します。

- ネットワークトラフィックをモニタし、定義されたルールセットに照らしあわせて分析します。
- 攻撃の分類を行います。
- 一致したルールに照らしあわせてアクションを呼び出します。

要件に応じて、IPS または IDS モードで Snort を有効にできます。IDS モードでは、Snort はトラフィックを検査し、アラートを報告しますが、攻撃を防ぐためのアクションは実行しません。IPS モードでは、侵入検知に加えて、攻撃を防ぐためのアクションを実行します。

Snort IPS はトラフィックをモニタし、イベントを外部ログサーバまたは IOS syslog に報告します。IOS syslog へのロギングを有効にすると、ログメッセージが大量に発生する可能性があるため、パフォーマンスに影響する場合があります。Snort ログに対応する外部のサードパーティ製のモニタリングツールを、ログの収集と分析に使用できます。

# Snort IPS ソリューション

Snort IPS ソリューションは、次のエンティティで構成されています。

- Snort センサー：トラフィックをモニタして、設定されたセキュリティポリシー（署名、統計情報、プロトコル分析など）に基づいて異常を検出し、アラートサーバまたはレポートサーバにアラートメッセージを送信します。Snort センサーは、仮想コンテナサービスとしてルータに導入されます。
- 署名ストア：定期的に更新される Cisco 署名パッケージをホストします。これらの署名パッケージは、定期的にもしくはオンデマンドで Snort センサーにダウンロードされます。検証済みの署名パッケージは Cisco.com に掲載されます。設定に基づいて、署名パッケージを Cisco.com またはローカルサーバからダウンロードできます。

  注　署名パッケージを保持するためにローカルサーバから署名パッケージをダウンロードする場合は、HTTP のみに対応します。

  Snort センサーが署名パッケージを取得するには、Cisco.com の認証情報を使用して、署名パッケージを Cisco.com からローカルサーバに手動でダウンロードする必要があります。

  URL が IP アドレスとして指定されていない場合、Snort コンテナは（ルータに設定された DNS サーバ上で）ドメイン名ルックアップを実行して、Cisco.com によるまたはローカルサーバ上の自動署名更新の場所を解決します 。
- アラートまたはレポートサーバ：Snort センサーからアラートイベントを受信します。Snort センサーによって生成されたアラートイベントは、IOS syslog または外部 syslog サーバ、もしくは IOS syslog と外部 syslog サーバの両方に送信できます。Snort IPS ソリューションに付属している外部ログサーバはありません。
- 管理：Snort IPS ソリューションを管理します。管理は、IOS CLI を使用して設定します。Snort センサーには直接アクセスできず、すべての設定は IOS CLI を使用してのみ行えます。

# Snort 仮想サービスインターフェイスの概要

Snort センサーは、ルータ上でサービスとして動作します。サービスコンテナは、仮想テクノロジーを使用して、アプリケーション用の Cisco デバイスにホスティング環境を提供します。

Snort トラフィック検査は、インターフェイス単位で、または対応しているすべてのインターフェイスでグローバルに有効にできます。検査対象のトラフィックは Snort センサーに転送され、再度投入されます。侵入検知システム（IDS）では、識別された脅威がログイベントとして報告され、許可されます。ただし、侵入防止システム（IPS）では、ログイベントとともに攻撃を防ぐためのアクションが実行されます。

Snort センサーには 2 つの VirtualPortGroup インターフェイスが必要です。最初の VirtualPortGroup インターフェイスは管理トラフィックに使用され、2 つ目は転送プレーンと Snort 仮想コンテナサービス間のデータトラフィックに使用されます。これらの VirtualPortGroup インターフェイスには、ゲスト IP アドレスを設定する必要があります。管理 VirtualPortGroup インターフェイスに割り当てられた IP サブネットは、署名サーバおよびアラート / 報告サーバと通信できる必要があります。

2 つ目の VirtualPortGroup インターフェイスの IP サブネットは、このインターフェイス上のトラフィックがルータ内部にあるため、カスタマーネットワーク上でルーティング可能であってはなりません。内部サブネットを外部に公開することはセキュリティ上のリスクとなります。2 つ目の VirtualPortGroup サブネットには 192.0.2.0/30 の IP アドレス範囲を使用することをお勧めします。192.0.2.0/24 のサブネットを使用することは、RFC 3330 で定義されています。

仮想サービスが実行されているルータと同じ管理ネットワークで、Snort 仮想コンテナサービスの IP アドレスを割り当てることができます。この設定は、syslog またはアップデートサーバが管理ネットワーク上にあり、他のインターフェイスからアクセスできない場合に役立ちます。

# 統合脅威防御（UTD）のマルチテナントの設定に関する制約事項

- 統合脅威防御（UTD）のマルチテナントは、Cisco CSR 1000v にのみ対応します。
- ドメインベースのフィルタリングには対応しません。
- 各 Cisco CSR 1000v インスタンスで最大25のテナントに対応します。
- 最大 25 のポリシーに対応します。
- Cisco CSR 1000v では、最大 50,000 の同時セッションに対応します。
- 脅威検知で設定されたポリシーの数に応じて、Snort IPS または IDS パッケージの起動（またはリロードおよび更新）に最大 20 分かかることがあります。署名を更新すると、Snort IPS がリロードされ、これは最大 20 分かかります。

- ブロックリストまたは許可リストのルールは、正規表現のパターンのみに対応します。現在、ブロックリストまたは許可リストのルールごとに 64 のパターンに対応しています。ただし、各テナントには複数のルールを設定できます。
- ローカルブロックサーバは、HTTPS ブロックページの提供には対応していません。URL フィルタがブロックページまたはリダイレクトメッセージを挿入しようとする場合、HTTPS トラフィックには対応しません。
- URL にユーザ名とパスワードがある場合、ブロックリストまたは許可リストのパターンと一致する前に、URL フィルタがユーザ名とパスワードを URL から削除することはしません。ただし、カテゴリまたはレピュテーションルックアップにはこの制限はなく、ルックアップの前に URL からユーザ名とパスワードを削除します。
- HTTPS 検査は制限されています。Web フィルタリングでは、サーバ証明書を使用して URL およびドメイン情報を取得します。完全な URL のパスを検査することはできません。
- UTD は、VRF 間シナリオにおいては WCCP および NBAR との相互運用は行いません。
- Snort IPS コマンドの `threat inspection profile` *`profile-name`* は、ID（番号）ではなく英数字のプロファイル名を使用します。

# 統合脅威防御（UTD）のマルチテナントの設定に関する前提条件

Cisco CSR 1000v で UTD 機能のマルチテナント機能を設定する前に、ルータが次のように設定されていることを確認します。

- Cisco CSR 1000v が Cisco IOS XE Everest 16.6.1 以降で動作している。
- Web フィルタリングを有効にするには、Cisco CSR 1000v にセキュリティ K9 ライセンスが必要である。
- Cisco CSR 1000v の「マルチテナント」プロファイルには、次の仮想サービスシステム CPU、仮想サービスメモリ、およびプラットフォーム要件が必要である。

  システム CPU：25%

  プラットフォームのメモリ要件：最小 12 GB RAM（8 GB ディスクまたはフラッシュ）

# 統合脅威防御（UTD）のマルチテナントの設定方法

対応しているデバイスに Unified Threat Defense のマルチテナント機能を導入するには、次のタスクを実行します。

### 始める前に

マルチテナント用に Web フィルタリングおよび脅威検知をインストールするデバイスをプロビジョニングします。この機能は現在、Cisco CSR 1000v でのみ対応しています。

ライセンスを取得します。UTD は、セキュリティパッケージを実行しているルータでのみ使用でき、サービスを有効にするにはセキュリティライセンスが必要となります。セキュリティライセンスの取得については、シスコサポートにお問い合わせください。

### 手順の概要

1. 仮想サービスをインストールしてアクティブにします。マルチテナント用の UTD OVA ファイルのインストール （102 ページ）
2. VirtualPortGroup のインターフェイスおよび仮想サービスを設定します。マルチテナント用の VirtualPortGroup インターフェイスと仮想サービスの設定方法 （103 ページ）
3. VRF を設定します。マルチテナント用の VRF の設定方法 （106 ページ）
4. マルチテナント用の脅威検知と Web フィルタリングを設定します。マルチテナント Web フィルタリングおよび脅威検知の設定方法 （107 ページ）

### 手順の詳細

**ステップ 1** 仮想サービスをインストールしてアクティブにします。マルチテナント用の UTD OVA ファイルのインストール （102 ページ）

**ステップ 2** VirtualPortGroup のインターフェイスおよび仮想サービスを設定します。マルチテナント用の VirtualPortGroup インターフェイスと仮想サービスの設定方法 （103 ページ）

**ステップ 3** VRF を設定します。マルチテナント用の VRF の設定方法 （106 ページ）

**ステップ 4** マルチテナント用の脅威検知と Web フィルタリングを設定します。マルチテナント Web フィルタリングおよび脅威検知の設定方法 （107 ページ）

# マルチテナント用の UTD OVA ファイルのインストール

仮想サービスの OVA ファイルは、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ファイルです。この OVA ファイルをルータにダウンロードしてから、仮想サービスをインストールする必要があります。仮想サービスの OVA ファイルは、ルータにインストールされている Cisco IOS XE リリースイメージには付属していません。OVA ファイルは、ルータのフラッシュメモリに事前にインストールされている場合があります。

OVA ファイルをインストールするには、セキュリティライセンス付きの Cisco IOS XE イメージを使用する必要があります。インストール中に、セキュリティライセンスのチェックが行われます。

仮想サービスのインストール例：

```
Device> enable
Device# virtual-service install name utd package
bootflash:utdsnort.1.0.4_SV2983_XE_16_6.20170623_174453_RELEASE.ova
Device# show virtual-service list

Name Status   Package Name
------------------------------------------------------------------------------
utd Activated utdsnort.1.0.4_SV2983_XE_16_6.20170
```

仮想サービスのアップグレードの例：

```
Device> enable
Device# virtual-service upgrade name utd package
bootflash:utdsnort.1.0.4_SV2983_XE_16_6.20170623_174453_RELEASE.ova
Device# show virtual-service list

Name Status   Package Name
------------------------------------------------------------------------------
utd Activated utdsnort.1.0.4_SV2983_XE_16_6.20170
```

仮想サービスのアンインストールの例：

```
Device> enable
Device# virtual-service uninstall name utd
Device# show virtual-service list

Virtual Service List:
```

# マルチテナント用のVirtualPortGroupインターフェイスと仮想サービスの設定方法

この手順に示すように、マルチテナントの場合、2 つの VirtualPortGroup インターフェイスと両方のインターフェイスのゲスト IP アドレスを設定する必要があります。

（注） データトラフィック用の VirtualPortGroup インターフェイスは、プライベートまたはルーティング不可の IP アドレスを使用する必要があります。このインターフェイスには、IP アドレスの範囲として 192.0.2.0 / 30を 使用することを推奨します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface VirtualPortGroup** *interface-number*
4. **ip address** *ip-address mask*
5. **exit**
6. **interface VirtualPortGroup** *interface-number*
7. **ip address** *ip-address mask*
8. **exit**
9. **virtual-service** *name*
10. **profile multi-tenancy**

11. **vnic gateway VirtualPortGroup** *interface-number*
12. **guest ip address** *ip-address*
13. **exit**
14. **vnic gateway VirtualPortGroup** *interface-number*
15. **guest ip address** *ip-address*
16. **exit**
17. **activate**
18. **end**
19. **show virtual-service list**

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**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Device# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **interface VirtualPortGroup** *interface-number*<br>例：<br>`Device(config)# interface VirtualPortGroup 0` | インターフェイス設定モードに入り、VirtualPortGroup インターフェイスを設定します。このインターフェイスは、管理インターフェイスの GigabitEthernet0 が使用されていない場合に管理トラフィックに対して使用されます。 |
| ステップ 4 | **ip address** *ip-address mask*<br>例：<br>`Device(config-if)# ip address 10.1.1.1 255.255.255.252` | インターフェイスのプライマリ IP アドレスを設定します。このインターフェイスは、署名アップデートサーバおよび外部ログサーバにルーティング可能である必要があります。 |
| ステップ 5 | **exit**<br>例：<br>`Device(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 | **interface VirtualPortGroup** *interface-number*<br>例：<br>`Device(config)# interface VirtualPortGroup 1` | インターフェイスを設定し、インターフェイス設定モードを開始します。VirtualPortGroup インターフェイスを設定します。このインターフェイスは、データトラフィックに使用されます。 |
| ステップ 7 | **ip address** *ip-address mask*<br>例：<br>`Device(config-if)# ip address 192.0.2.1 255.255.255.252` | インターフェイスのプライマリ IP アドレスを設定します。この IP アドレスは、外部ネットワークに対してルーティング不能である必要があります。IP アドレスは、推奨される 192.0.2.0/30 のサブネットから割り当てられます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 8 | **exit**<br>例：<br>`Device(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 9 | **virtual-service** *name*<br>例：<br>`Device(config)# virtual-service utd` | 仮想コンテナサービスを設定し、仮想サービス設定モードに入ります。*name* 引数は、仮想コンテナサービスを識別するために使用される論理名です。 |
| ステップ 10 | **profile multi-tenancy**<br>例：<br>`Device(config-virt-serv)#profile multi-tenancy` | リソースプロファイルを設定します。マルチテナントモードの場合（Cisco CSR 1000v のみ）、このプロファイル マルチテナント コマンド を設定する必要があります。 |
| ステップ 11 | **vnic gateway VirtualPortGroup** *interface-number*<br>例：<br>`Device(config-virt-serv)# vnic gateway VirtualPortGroup 0` | 仮想サービスの仮想ネットワーク インターフェイス カード（vNIC：virtual network interface card）設定モードに入ります。仮想コンテナサービス用の vNIC ゲートウェイ インターフェイスを作成し、vNIC ゲートウェイ インターフェイスを仮想ポート グループ インターフェイスにマッピングします。これは、手順 3 で設定したインターフェイスです。 |
| ステップ 12 | **guest ip address** *ip-address*<br>例：<br>`Device(config-virt-serv-vnic)# guest ip address 10.1.1.2` | vNIC ゲートウェイ インターフェイスのゲスト vNIC アドレスを設定します。 |
| ステップ 13 | **exit**<br>例：<br>`Device(config-virt-serv-vnic)# exit` | 仮想サービスの vNIC 設定モードを終了し、仮想サービス設定モードに戻ります。 |
| ステップ 14 | **vnic gateway VirtualPortGroup** *interface-number*<br>例：<br>`Device(config-virt-serv)# vnic gateway VirtualPortGroup 1` | 仮想サービスの vNIC 設定モードに入ります。仮想コンテナサービス用の vNIC ゲートウェイ インターフェイスを設定し、インターフェイスを仮想ポート グループにマッピングします。手順 6 で設定されたインターフェイス（*interface-number*）は、ユーザトラフィックをモニタするために Snort エンジンによって使用されます。 |
| ステップ 15 | **guest ip address** *ip-address*<br>例：<br>`Device(config-virt-serv-vnic)# guest ip address 192.0.2.2` | vNIC ゲートウェイ インターフェイスのゲスト vNIC アドレスを設定します。 |
| ステップ 16 | **exit**<br>例： | 仮想サービスの vNIC 設定モードを終了し、仮想サービス設定モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config-virt-serv-vnic)# exit` | |
| ステップ 17 | **activate**<br>例：<br>`Device(config-virt-serv)# activate` | 仮想コンテナサービスにインストールされたアプリケーションをアクティブにします。 |
| ステップ 18 | **end**<br>例：<br>`Device(config-virt-serv)# end` | 仮想サービス設定モードを終了し、特権EXECモードに戻ります。 |
| ステップ 19 | **show virtual-service list**<br>例：<br>`Device# show virtual-service list`<br><br>`Virtual Service List:`<br><br>`Name Status Package Name`<br>`---`<br>`utd Activated utdsnort.1.0.4_SV2983_XE_16_6.20170` | |

# マルチテナント用の VRF の設定方法

この手順では、テナントの VRF を設定するために必要な一般的な手順について説明します。この手順は後にマルチテナント Web フィルタリングおよび脅威検知の設定方法 （107 ページ）で使います。

（注） VRF 間トラフィックの場合、2 つの VRF 間を流れるトラフィックに UTD 用の入力インターフェイスと出力インターフェイスが設定されている場合、セッションを表す VRF を決定するルールが適用されます。選択した VRF の UTD ポリシーは、VRF 間トラフィックのすべてのパケットに適用されます。

## 手順の概要

1. **vrf definition** *vrf-name*
2. **rd** *route-distinguisher*
3. **address-family ipv4**
4. **exit address-family**
5. VRF ごとに手順 1 ～ 4 を繰り返します。

手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **vrf definition** *vrf-name*<br>例：<br>`Device(config)# vrf definition 100` | VRF 名を定義し、VRF 設定モードに入ります。 |
| ステップ 2 | **rd** *route-distinguisher*<br>例：<br>`Device(config-vrf)# rd 100:1` | ルーティングテーブルと転送テーブルを作成し、ルート識別子を「VRF 名」という名前の VRF インスタンスに関連付けます。ルータはルート識別子を使用して、パケットが属する VRF を識別します。ルート識別子は、次の 2 つのタイプのいずれかとなります。<br>• 自律システム関連。AS 番号 xxx および任意の番号 y：xxx:y<br>• IP アドレス関連。IP アドレス A.B.C.D および任意の番号 y：A.B.C.D:y |
| ステップ 3 | **address-family ipv4**<br>例：<br>`Device(config-vrf)# address-family ipv4` | IP バージョン 4 アドレスを使用してルーティングセッションを設定するためのアドレスファミリ設定モードに入ります。 |
| ステップ 4 | **exit address-family**<br>例：<br>`Device(config-vrf-af)# exit` | アドレスファミリ設定モードを終了します。 |
| ステップ 5 | VRF ごとに手順 1 ～ 4 を繰り返します。 | |

# マルチテナント Web フィルタリングおよび脅威検知の設定方法

マルチテナント（複数のテナントまたは VRF）の脅威検知（IPS または IDS）および Web フィルタリングを設定するには、次の手順を実行します。

この手順では、ブロックリストと許可リストの定義を最初の手順 1 ー 5 に示します。主な設定手順（マルチテナント用の UTD 標準エンジンの設定モード）は、手順 6 以降に示しています。

（注） シングルテナント用の脅威検知と Web フィルタリングの詳細については、Snort IPS （23 ページ） および Web フィルタリング （75 ページ） を参照してください。

### 始める前に

`no utd engine standard` コマンドを使用して、既存のシングルテナントの UTD 設定を削除します。

テナントごとに VRF を事前に設定しておく必要があります（マルチテナント用の VRF の設定方法 （106 ページ） を参照）。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **parameter-map type regex** *blacklist-name*<br>例：<br>`Device(config)# parameter-map type regex urlf-blacklist1` | ブロックリストのパラメータマップを定義します。これは、後に手順 17 で使用します。 |
| ステップ 2 | **pattern** *URL-name*<br>例：<br>`Device(config-profile)# pattern www\.cnn\.com`<br>`Device(config-profile)# pattern www\.msnbc\.com` | ブロックリストに登録する URL を定義します。*URL-name* 内のピリオドの前には、必ずエスケープ「\」文字を入れてください。ブロックリストに複数の URL を設定するには、この手順を繰り返します。 |
| ステップ 3 | **parameter-map type regex** *whitelist-name*<br>例：<br>`Device(config-profile)# parameter-map type regex urlf-whitelist1` | 許可リストのパラメータマップを定義します。これは、後に手順 20 で使用します。 |
| ステップ 4 | **pattern** *URL-name*<br>例：<br>`Device(config-profile)# pattern www\.nfl\.com` | 許可リストに登録する URL を定義します。ブロックリストの URL では、*URL-name* 内のピリオドの前には、必ずエスケープ「\」文字を入れてください。許可リストに複数の URL を設定するには、この手順を繰り返します。 |
| ステップ 5 | **exit**<br>例：<br>`Device(config-profile)# exit` | |
| ステップ 6 | **utd multi-tenancy**<br>例：<br>`Device(config)# utd multi-tenancy` | このコマンドは、次の `utd engine standard multi-tenancy` コマンドに備えて、スイッチの役割を果たします。 |
| ステップ 7 | **utd engine standard multi-tenancy**<br>例： | マルチテナント用の UTD 標準エンジンの設定モードに入ります。 |

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td></td><td><pre>Device(config)# utd engine standard multi-tenancy</pre></td><td>（注） 後に手順 50 で UTD 標準エンジンの設定モードを終了すると、ポリシー設定が適用されます。</td></tr>
<tr><td>ステップ 8</td><td>web-filter sourcedb sourcedb-number<br>例：<br><pre>Device(config)# web-filter sourcedb 1</pre></td><td>Web フィルタリングのソース DB プロファイル（sourcedb-number は数字）を設定します。これは、後に手順 29 で使用されます。</td></tr>
<tr><td>ステップ 9</td><td>logging level {alerts | critical | debugging | emergencies | errors | informational | notifications | warnings}<br>例：<br><pre>Device(config)# logging level errors</pre></td><td>Web フィルタリングイベントに関して報告されるシステムメッセージのレベルを設定します。指定したレベル以下のメッセージが報告されます。（各レベルには、次の表に示す数値があります）<br>表 5: システム メッセージの重大度<table><tr><th>レベル</th><th>説明</th></tr><tr><td>0：emergencies</td><td>システムが使用不可</td></tr><tr><td>1：alerts</td><td>即時処理が必要</td></tr><tr><td>2：critical</td><td>クリティカル状態</td></tr><tr><td>3：errors</td><td>エラー状態</td></tr><tr><td>4：warnings</td><td>警告状態</td></tr><tr><td>5：notifications</td><td>正常だが注意を要する状態</td></tr><tr><td>6：informational</td><td>情報メッセージだけ</td></tr><tr><td>7：debugging</td><td>デバッグ実行時にのみ表示</td></tr></table></td></tr>
<tr><td>ステップ 10</td><td>web-filter block local-server profile profile-id<br>例：<br><pre>Device(config-utd-multi-tenancy)# web-filter block local-server profile 1</pre>コンテンツのテキストはローカルサーバによって表示されます。</td><td>Webフィルタリングのローカルブロックサーバのプロファイルを設定します。profile-id の値の範囲は 1 ー 255 です。<br>「ローカルブロックサーバを使用した URL ベースの Web フィルタリングの設定」を参照してください。<br>（注） マルチテナント用のコマンドを設定する場合、シングルテナントと比較して、最初の <code>utd</code> というキーワードを使用しないでください。</td></tr>
</table>

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 11 | **block-page-interface loopback** *id*<br>例：<br>`Device(config-utd-mt-webf-blk-srvr)# block-page-interface loopback 110` | ループバックインターフェイスにこのプロファイルを関連付けます。このループバックインターフェイスの IP アドレスは、ブロックローカルサーバの IP アドレスとして使用されます。 |
| ステップ 12 | **content text** *display-text*<br>例：<br>`Device(config-utd-mt-webf-blk-srvr)# content text "Blocked by Web-Filter"` | ブロックされたページにアクセスした後に表示される警告テキストを指定します。 |
| ステップ 13 | **http-ports** *port-number*<br>例：<br>`Device(config-utd-mt-webf-blk-srvr)# http-ports 80` | http ポート値は、カンマで区切られたポートの文字列です。nginx HTTP サーバはこれらのポートをリッスンします。 |
| ステップ 14 | **web-filter block page profile** *profile-name*<br>例：<br>`Device(config-utd-multi-tenancy)# web-filter block page profile 1`<br>`Device(config-utd-mt-webf-block-urc)# text "this page is blocked"` | インラインブロックページを使用した URL ベースの Web フィルタリングの設定 （88 ページ） を参照してください。ただし、マルチテナント用にここで使用されるコマンドは、シングルテナント用に使用される `utd` キーワードを使用しません）。 |
| ステップ 15 | **web-filter url profile** *web-filter-profile-id*<br>例：<br>`Device(config-utd-multi-tenancy)# web-filter url profile 1`<br>`Device(config-utd-mt-webfltr-url)#` | Web フィルタリングの URL プロファイルである *web-filter-profile-id* を指定します。値は 1 ～ 255 です。このコマンドの後、ブロックリスト、許可リスト、およびカテゴリのアラートを設定できます。詳細については、「インラインブロックページを使用した URL ベースの Web フィルタリングの設定」を参照してください。<br>（注） マルチテナント用のコマンドを設定する場合、シングルテナントと比較して、最初の `utd` というキーワードを使用しないでください。 |
| ステップ 16 | **blacklist**<br>例：<br>`Device(config-utd-mt-webfltr-url)# blacklist` | Web フィルタリングのブロックリストの設定モードに入ります。 |
| ステップ 17 | **parameter-map regex** *blacklist-name*<br>例：<br>`Device(config-utd-mt-webf-url-bl)# parameter-map regex urlf-blacklist1` | 手順 1 で前に定義したブロックリストを使用して、パラメータマップの正規表現を指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 18 | **exit**<br>例：<br>`Device(config-utd-mt-webf-url-bl)# exit`<br>`Device(config-utd-mt-webfltr-url)#` | Web フィルタリングのブロックリストの設定モードを終了します。 |
| ステップ 19 | **whitelist**<br>例：<br>`Device(config-utd-mt-webfltr-url)# whitelist`<br>`Device(config-utd-mt-webf-url-wl)#` | Web フィルタリングの許可リストの設定モードに入ります。 |
| ステップ 20 | **parameter-map regex** *whitelist-name*<br>例：<br>`Device(config-utd-mt-webf-url-wl)# parameter-map regex urlf-list1` | 手順3で前に定義した許可リストを使用して、パラメータマップの正規表現を指定します。 |
| ステップ 21 | **exit**<br>例：<br>`Device(config-utd-mt-webf-url-wl)# exit`<br>`Device(config-utd-mt-webfltr-url)#` | Web フィルタリングの許可リストの設定モードを終了します。 |
| ステップ 22 | **exit**<br>例：<br>`Device(config-utd-mt-webfltr-url)# exit`<br>`Device(config-utd-multi-tenancy)#` | Web フィルタリングの URL プロファイルモードを終了します。 |
| ステップ 23 | **utd global**<br>例：<br>`Device(config-utd-multi-tenancy)# utd global` | `utd global` に入力されたコマンドは、すべてのテナントまたはポリシーに適用されます。Cisco CSR 1000v インスタンスの場合のコマンド例は、`logginghost syslog` および `threat inspection` などです。 |
| ステップ 24 | **logging** {**host** *hostname* \| **syslog**}<br>例：<br>この例では、アラートは指定されたホストのログファイルに記録されます。<br>`Device(config-utd-mt-utd-global)# logging host systemlog1`<br>例：<br>この例では、アラートは IOS syslog に記録されます。<br>`Device(config-utd-mt-utd-global)# logging syslog` | `logging` コマンドは、syslog メッセージの送信先となるホスト名または IOS syslog を指定します。 |
| ステップ 25 | **threat inspection**<br>例： | グローバル脅威検知モードに入ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config-utd-mt-utd-global)# threat inspection` | |
| ステップ 26 | **signature update server** {**cisco** \| **url** *url* } [**username** *username* [**password** *password*]]<br>例：<br>`Device(config-utd-mt-utd-global-threat)# signature update server cisco username abcd password cisco123` | 署名更新サーバのパラメータを設定します。サーバの詳細で署名更新パラメータを指定する必要があります。署名の更新に www.cisco.com を使用する場合は、ユーザ名とパスワードを入力する必要があります。署名の更新にローカルサーバを使用する場合は、サーバ設定に基づいてユーザ名とパスワードを指定できます。ルータは、インターネットに接続することでドメイン名を解決できる必要があります。 |
| ステップ 27 | **signature update occur-at** {**daily** \| **monthly** *day-of-month* \| **weekly** *day-of-week*} *hour minute*<br>例：<br>`Device(config-utd-mt-utd-global-threat)# signature update occur-at daily 0 0` | 署名の更新間隔パラメータを設定します。この設定をすることで、午前0時に署名の更新がトリガーされます。 |
| ステップ 28 | **web-filter**<br>例：<br>`Device(config-utd-mt-utd-global-threat)# web-filter` | このコマンドは、次の `sourcedb` コマンドと組み合わせて使用し、Web フィルタリングの URL ソースデータベースを指定します。 |
| ステップ 29 | **sourcedb** *sourcedb-number*<br>例：<br>`Device(config-utd-mt-utd-global-threat)# sourcedb 1` | Web フィルタリングのソースデータベースを割り当てます。アクティブにできるソースデータベースは 1 つだけです。 |
| ステップ 30 | **exit**<br>例：<br>`Device(config-utd-mt-utd-global-threat)# exit` | 脅威検知設定モードを終了します。 |
| ステップ 31 | **exit**<br>例：<br>`Device(config-utd-mt-global)# exit` | グローバル更新設定モードを終了します。 |
| ステップ 32 | **threat-inspection list profile** *policy-name*<br>例：<br>`Device(config-utd-multi-tenancy)# threat-inspection list profile wh101` | 許可リストのプロファイルを現在設定されているポリシーに関連付けます。同様のコマンドがシングルテナントで使用されますが、`utd` キーワードを使用します。 |
| ステップ 33 | **signature id** *id*<br>例：<br>`Device(config-utd-mt-list)# signature id 101` | 以前に脅威として特定した ID である *id* を指定します。たとえば、アラートのログファイルの ID を確認した後などです。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 複数の署名 ID に対してこのコマンドを繰り返します。 |
| ステップ 34 | **exit**<br>例：<br>`Device(config-utd-mt-whitelist)# exit` | 許可リストの設定モードを終了します。 |
| ステップ 35 | **threat-inspection profile** *profile-name*<br>例：<br>`Device(config-utd-multi-tenancy)# threat-inspection profile 101` | 脅威検知プロファイルを設定することで、複数のテナントにより再利用できるようになります。複数の脅威検知プロファイルを設定できます。プロファイル内では、複数の許可リストを設定できます。<br>`profile-name` は英数字です。 |
| ステップ 36 | **threat** {**detection** \| **protection** }<br>例：<br>`Device(config-utd-mt-threat)# threat protection` | Snort エンジンの動作モードとして侵入検知システム（IDS）または侵入防止システム（IPS）を指定します。<br>デフォルトは **threat detection** です。 |
| ステップ 37 | **policy** {**balanced** \| **connectivity** \| **security**}<br>例：<br>`Device(config-utd-mt-threat)# policy security` | Snort エンジンのセキュリティポリシーを設定します。<br>• デフォルトのセキュリティポリシータイプは **balanced** です。 |
| ステップ 38 | **logging level**{**alert** \| **crit** \| **debug** \| **emerg** \| **err** \| **info** \| **notice** \| **warning**} | 次のいずれかのカテゴリのログを表示します。<br>• alert：アラートレベルのログを表示します（重大度 = 2）。<br>• crit：クリティカルレベルのログ（重大度 = 3）<br>• debug：すべてのログ（重大度 = 8）<br>• emerg：緊急レベルのログ（重大度 = 1）<br>• err：エラーレベルのログ（重大度 = 4）デフォルト。<br>• info：情報レベルのログ（重大度 = 7）<br>• notice：通知レベルのログ（重大度 = 6）<br>• warning：警告レベルのログ（重大度 = 5） |
| ステップ 39 | **whitelist profile** *profile-name*<br>例：<br>`Device(config-utd-mt-threat)# whitelist profile wh101` | また、許可リストプロファイルを別の場所にある許可リストのプロファイルに対してのみ指定することもできます（上記の `threat-inspection whitelist profile` コマンド）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | （オプション）UTD エンジンで許可リストを有効にします。 |
| ステップ 40 | **exit**<br>例：<br>`Device(config-utd-mt-threat)# exit` | 脅威検知モードを終了します。 |
| ステップ 41 | 脅威検知プロファイルを追加するには、手順 35 ー 40 を繰り返します。 | |
| ステップ 42 | **policy** *policy-name*<br>例：<br>`Device(config-utd-multi-tenancy)# policy pol101` | 複数のテナントに関連付けるポリシーを定義します。脅威検知（IPS）および Web フィルタリングのプロファイルがポリシーに追加されます。 |
| ステップ 43 | **vrf** [ *vrf-name* \| global ]<br>例：<br>この例では、2 つのテナント（VRF）と 2 つのポリシーの設定を示します。<br>`Device(config-utd-mt-policy)# vrf vrf101` | UTD ポリシーを使用する VRF（テナント）ごとに `vrf vrf-name` コマンドを繰り返し入力します。以前に定義されたこれらの VRF については、マルチテナント用の VRF の設定方法 （106 ページ） を参照してください。<br>または、`vrf global` を使用してグローバル（デフォルト）VRF に関連付け、インターフェイスで VRF を有効にします。 |
| ステップ 44 | **all-interfaces**<br>例：<br>`Device(config-utd-mt-policy)# all-interfaces` | （オプション）VRF のすべてのインターフェイスをポリシーに関連付けます。 |
| ステップ 45 | **threat-inspection profile** *profile-name*<br>例：<br>`Device(config-utd-mt-policy)# threat-inspection profile 101` | （オプション）以前に定義した脅威検知プロファイルにポリシーを関連付けます。手順 35 を参照してください。 |
| ステップ 46 | **web-filter url profile** *web-filter-profile-id*<br>例：<br>`Device(config-utd-mt-policy)# web-filter url profile 1` | （オプション）以前に定義した Web フィルタリングのプロファイルにポリシーを関連付けます。手順 15 を参照してください。 |
| ステップ 47 | **fail close**<br>例：<br>`Device(config-utd-mt-policy)# fail close` | （オプション）エンジン障害時に IPS または IDS パケットをドロップします。デフォルトは `fail open` です。 |
| ステップ 48 | **exit** | ポリシー設定モードを終了します。 |
| ステップ 49 | 各ポリシーに対して手順 42 ー 48 を繰り返します。 | |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 50 | **exit**<br>例：<br>`Device(config-utd-multi-tenancy)# exit` | `utd engine standard multi-tenancy`モードを終了します。<br>ポリシー設定が適用されます。これには数分かかる場合があります。この間は、`utd engine standard multi-tenancy`設定モードのコマンドはそれ以上入力できません。 |
| ステップ 51 | **exit**<br>例：<br>`Device(config)# exit`<br>`Device#` | |
| ステップ 52 | **show logging**<br>例：<br>`Device(config)# show logging`<br>`..UTD MT configuration download has started`<br>`..UTD MT configuration download has completed` | （オプション）ポリシー設定が適用されているかどうかを確認するログメッセージを表示します。次のようなメッセージを検索します。<br>`..UTD MT configuration download has started`<br>`..UTD MT configuration download has completed`<br>「`download has completed`」を含むメッセージは、ポリシー設定が適用されたことを示します。 |
| ステップ 53 | **interface** *sub-interface*<br>例：<br>`Device(config)# interface GigabitEthernet4.101` | テナント（VRF）に使用するサブインターフェイスを指定します。 |
| ステップ 54 | **encapsulation dot1Q** *vlan-id*<br>例：<br>`Device(config-if)# encapsulation dot1Q 101` | VLAN ID をサブインターフェイスに適用します。 |
| ステップ 55 | **ip vrf forwarding** *vrf-name*<br>例：<br>`Device(config-if)# ip vrf forwarding vrf101` | VRF インスタンスをサブインターフェイスに関連付けます。 |
| ステップ 56 | **ip address** *ip-address subnet-mask*<br>例：<br>`Device(config-if)# ip address 111.0.0.1 255.255.255.0` | VRF のサブインターフェイスの IP アドレスを指定します。 |
| ステップ 57 | **ip route** *ip-address subnet-mask sub-interface*<br>例：<br>この例では、VRF のサブネット GigabitEthernet4.101 は、静的 IP アドレス 111.0.0.0 255.255.255.0 を使用 | （オプション）次の手順のこの `ip route` コマンドと `ip route vrf` コマンドはオプションです。VRF とグローバル ルーティング テーブル間の静的ルートを使用してルートリークを設定する場合にこれらの手順を使用できます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | してグローバル ルーティング テーブルにリンクされています。<br>`Device(config-if)# ip route 111.0.0.0 255.255.255.0 GigabitEthernet4.101` | これにより、VRF インターフェイスから VRF サブネットへの静的ルートが設定され、VRF サブネットにグローバル ルーティング テーブルからアクセスできるようになります。ルートリークの設定の詳細については、「MPLS または VPN ネットワークでのルートリーク」を参照してください。 |
| ステップ 58 | **ip route vrf** *vrf-name ip-address subnet-mask* **global**<br>例：<br>`Device(config-if)# ip route vrf vrf101 0.0.0.0 0.0.0.0 5.2.1.1 global` | （オプション）この手順と前の手順は任意となります。VRF とグローバル ルーティング テーブル間の静的ルートを使用してルートリークを設定する場合は、次の手順を使用できます。ルートリークの設定の詳細については、「MPLS または VPN ネットワークでのルートリーク」を参照してください。<br>グローバル ルーティング テーブルへの静的 VRF のデフォルトルートを指定します。 |
| ステップ 59 | **utd enable** | （オプション）インターフェイス上で UTD を有効にします。このコマンドは、`all-interfaces` コマンドが設定されていない場合に使用できます（手順 44 内）。 |
| ステップ 60 | 各テナント（VRF）のサブインターフェイスを設定するには、手順 53 ー 59 を繰り返します。 | |
| ステップ 61 | **exit** | インターフェイス設定モードを終了します。 |

Web フィルタリングおよび脅威検知（IPS）のプロファイルが適用されました。

# 設定例：統合脅威防御（UTD） のマルチテナント

この例は、2 つのテナントの UTD にマルチテナントを設定した後の一般的な実行設定を示しています。

（注） 次の例では、パラメータマップである `urlf-blacklist1` および `urlf-whitelist1` について説明します。これらのパラメータマップの設定は、例には示されていません。ブロックリストおよび承認済みリストのパラメータマップの詳細については、「インラインブロックページを使用した URL ベースの Web フィルタリングの設定」を参照してください。

```
utd multi-tenancy
utd engine standard multi-tenancy
 web-filter block page profile 1
  text "This page is blocked"
 web-filter block page profile 2
  text "This page is blocked"
 web-filter url profile 1
```

```
 alert all
 blacklist
  parameter-map regex urlf-blacklist1
 whitelist
  parameter-map regex urlf-whitelist1
 categories block
  social-network
  sports
 block page-profile 1
 log level error
web-filter url profile 2
 alert all
 blacklist
  parameter-map regex urlf-blacklist2
 categories block
  shopping
  news-and-media
  sports
  real-estate
  motor-vehicles
 block page-profile 2
 log level error
 reputation
  block-threshold low-risk
web-filter sourcedb 1
 logging level error
threat-inspection whitelist profile wh101
 signature id 101
threat-inspection profile 101
 threat protection
 policy security
 logging level debug
 whitelist profile wh101
threat-inspection profile 102
 threat detection
 policy security
 logging level debug
utd global
 logging host 172.27.58.211
 logging host 172.27.58.212
 logging host 172.27.56.97
 threat-inspection
  signature update server cisco username abc password
]RDCe[B\^KFI_LgQgCFeBEKWP^SWZMZMb]KKAAB
  signature update occur-at daily 0 0
 web-filter
  sourcedb 1
policy pol102
 vrf vrf102
 all-interfaces
 threat-inspection profile 102
 web-filter url profile 2
policy pol101
 vrf vrf101
 all-interfaces
 threat-inspection profile 101
 web-filter url profile 1
 fail close
```

# 統合脅威防御エンジンの標準設定の確認

次のコマンドを使用して、設定を確認します。

## 手順の概要

1. **enable**
2. **show utd multi-tenancy**
3. **show utd engine standard global**
4. **show utd engine standard status**
5. **show utd engine standard statistics**
6. **show utd engine standard statistics daq** [ **dp** | **cp** ]
7. **show utd engine standard statistics url-filtering** [ **engine** | *no* ]
8. **show utd engine standard statistics url-filtering vrf name** *vrf-name*
9. **show utd engine standard statistics internal**
10. **show utd engine standard logging event**
11. **show logging** | **include** CONFIG_DOWNLOAD
12. **show utd threat-inspection whitelist** [**profile** *profile-name*]
13. **show utd threat-inspection profile** *profile-name*
14. **show utd** [**policy** *profile-name*]
15. **show utd web-filter url** [**profile** *profile-name*]
16. **show utd web-filter block local-server** [**profile** *profile-name*]
17. **show utd web-filter sourcedb** [**profile** *profile-name*]
18. **show utd engine standard statistics daq dp** [**engine** *engine-num*] [**vrf** [**name** *vrf-name* | **global**]]
19. **show utd engine standard config threat-inspection whitelist** [**profile** *profile-name* ]
20. **show utd engine standard config web-filter url profile** *profile-name*
21. **show utd engine standard config** [**vrf name** *vrf-name* ]
22. **show utd engine standard config threat-inspection profile** *profile-name*
23. **show utd engine standard threat-inspection signature update status**
24. **show platform software qfp active feature utd config** [ **vrf**[ {**id** *vrf-id* | **name** *vrf-name* | **global** } ]
25. **show platform software utd interfaces**
26. **show platform hardware qfp active feature utd config** [**vrf** {**id** *vrf-id* | **name** *vrf-name* | **global** } ]
27. **show platform hardware qfp active feature utd stats** [**clear** | **divert** | **drop** | **general** | **summary**] [**vrf** {**id** *vrf-id* | **name** *vrf-name* | **global** }] [all] [**verbose**]
28. **show platform hardware qfp active feature utd stats summary** [**vrf name** *vrf-name* | **all**]
29. **show platform hardware qfp active feature utd stats drop all**

## 手順の詳細

ステップ 1　**enable**

例：

```
Device# 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　show utd multi-tenancy**

マルチテナントの現在のステータスを表示します。

**例**：

```
Device# show utd multi-tenancy
Multitenancy is enabled
```

**ステップ 3　show utd engine standard global**

UTD エンジン標準のグローバル設定を表示します。

**例**：

```
Device# show utd engine standard global
UTD Engine Standard Global: enabled
Threat-inspection: enabled
Web-filter: enabled
Logging:
```

**ステップ 4　show utd engine standard status**

UTD エンジンのステータスが緑色であることを確認します。

**例**：

```
Device# show utd eng standard status
Engine version       : 1.0.2_SV2983_XE_16_8

Profile              : Multi-tenancy
System memory        :
              Usage  : 3.50 %
              Status : Green
Number of engines    : 1

Engine        Running    CFT flows  Health     Reason
===============================================================
Engine(#1):   Yes        0          Green      None
===============================================================

Overall system status: Green

Signature update status:
========================
Current signature package version: 29.0.c
Last update status: Failed
Last successful update time: None
Last failed update time: Thu Jan 11 13:34:36 2018 PST
Last failed update reason: [Errno 113] No route to host
Next update scheduled at: None
Current status: Idle
```

**ステップ 5　show utd engine standard statistics**

**例**：

```
Device# show utd engine standard statistics
************Engine #1************
```

```
================================================================================
Memory usage summary:
Total non-mmapped bytes (arena): 80125952
Bytes in mapped regions (hblkhd): 359546880
Total allocated space (uordblks): 68314032
Total free space (fordblks): 11811920
Topmost releasable block (keepcost): 112
================================================================================
Packet I/O Totals:
Received: 49088
Analyzed: 49088 (100.000%)
Dropped: 0 ( 0.000%)
Filtered: 0 ( 0.000%)
Outstanding: 0 ( 0.000%)
Injected: 640
================================================================================
Breakdown by protocol (includes rebuilt packets):
Eth: 49394 (100.000%)

<output removed for brevity>

Total: 49394
================================================================================
Action Stats:
Alerts: 65 ( 0.132%)
Logged: 65 ( 0.132%)
Passed: 0 ( 0.000%)
```

**ステップ 6** **show utd engine standard statistics daq [ dp | cp ]**

Snort DAQ 統計情報を表示します。

**例**：

```
Device# show utd engine standard statistics daq dp
IOS-XE DAQ Counters(Engine #1):
----------------------------------
Frames received 654101
Bytes received 549106120
RX frames released 654101
Packets after vPath decap 654101
Bytes after vPath decap 516510928
Packets before vPath encap 651686
Bytes before vPath encap 514800669
Frames transmitted 651686
Bytes transmitted 544447557

<output removed for brevity>
```

**例**：

```
Device# show utd engine standard statistics daq cp
IOS-XE DAQ CP Counters(Engine #1):
------------------------------------
Packets received :16353210
Bytes received :1112018252
Packets transmitted :16353210
Bytes transmitted :1700733776
Memory allocation :16353212
Memory free :16353210
CFT API error :0
VPL API error :0
Internal error :0
```

```
External error :0
Memory error :0
Timer error :0
RX ring full 0
CFT full 0
sPath lib flow handle exhausted 0
Memory status changed to yellow :1
Memory status changed to red :0
Process restart notifications :0
```

**ステップ 7** **show utd engine standard statistics url-filtering** [ **engine** | *no* ]

すべてのテナントのURL統計情報（ブロックリストのサイトのヒット数、許可リストのサイトのヒット数、カテゴリブロックとレピュテーションブロックによってブロックされたサイトの数を）を表示します。

**例**：

```
Device# show utd engine standard statistics url-filtering
UTM Preprocessor Statistics
---------------------------
URL Filter Requests Sent:               377226166       379846771       381117940
URL Filter Response Received:           377009606       379622845       380892658
Blacklist Hit Count:                    0               0               0
Whitelist Hit Count:                    0               0               0

Reputation Lookup Count:                376859139       379458008       380706804
Reputation Action Block:                0               0               0
Reputation Action Pass:                 307             280             102
Reputation Action Default Pass:         376858832       379457728       380706702
Reputation Score None:                  376858832       379457728       380706702
Reputation Score Out of Range:          0               0               0

Category Lookup Count:                  376859139       379458008       380706804
Category Action Block:                  0               0               0
Category Action Pass:                   307             280             102
Category Action Default Pass:           376858832       379457728       380706702
Category None:                          376858832       379457728       380706702


Device# show utd engine standard statistics url-filtering engine1
UTM Preprocessor Statistics
-----------------------------------------------------
URL Filter Requests Sent:               377226166
URL Filter Response Received:           377009606
Blacklist Hit Count:                    0
Whitelist Hit Count:                    0

Reputation Lookup Count:                376859139
Reputation Action Block:                0
Reputation Action Pass:                 307
Reputation Action Default Pass:         376858832
Reputation Score None:                  376858832
Reputation Score Out of Range:          0

Category Lookup Count:                  376859139
Category Action Block:                  0
Category Action Pass:                   307
Category Action Default Pass:           376858832
Category None:                          376858832
```

**ステップ 8** **show utd engine standard statistics url-filtering vrf name** *vrf-name*

追加パラメータの **vrf name** *vrf-name* を使用して、テナントごとの URL の統計情報を表示します。

**例**：

```
Device# show utd engine standard statistics url-filtering vrf name vrf101
UTM Preprocessor Statistics
---------------------------
URL Filter Requests Sent: 764
URL Filter Response Received: 764
Blacklist Hit Count: 3
Whitelist Hit Count: 44

Reputation Lookup Count: 764
Reputation Action Block: 0
Reputation Action Pass: 58
Reputation Action Default Pass: 706
Reputation Score None: 706
Reputation Score Out of Range: 0

Category Lookup Count: 764
Category Action Block: 5
Category Action Pass: 53
Category Action Default Pass: 706
Category None: 706
```

**ステップ 9** **show utd engine standard statistics internal**

**例**：

```
Device# show utd engine standard statistics internal
*************Engine #1*************
===============================================================================
Memory usage summary:
Total non-mmapped bytes (arena): 80125952
Bytes in mapped regions (hblkhd): 359546880
Total allocated space (uordblks): 68314032
Total free space (fordblks): 11811920
Topmost releasable block (keepcost): 112
===============================================================================
Packet I/O Totals:
Received: 49088
Analyzed: 49088 (100.000%)
Dropped: 0 ( 0.000%)
Filtered: 0 ( 0.000%)
Outstanding: 0 ( 0.000%)
Injected: 640
===============================================================================
Breakdown by protocol (includes rebuilt packets):
Eth: 49394 (100.000%)
VLAN: 49394 (100.000%)
IP4: 49394 (100.000%)
Frag: 0 ( 0.000%)
ICMP: 5 ( 0.010%)
UDP: 2195 ( 4.444%)
TCP: 47194 ( 95.546%)

<output removed for brevity>
```

**ステップ 10** **show utd engine standard logging event**

VRF ごとにブロックリストまたは許可リストにあるアラートと URL を含むログを表示します。

**例**：

```
Device# show utd engine standard logging event

2017/08/04-16:01:49.205959 UTC [**] [Instance_ID: 1] [**] Drop [**]
UTD WebFilter Category/Reputation [**] [URL: www.cricinfo.com] ** [Category: Sports]
** [Reputation: 96] [VRF: vrf101] {TCP} 23.72.180.26:80 -> 111.0.0.254:53509
2017/08/04-16:02:12.253330 UTC [**] [Instance_ID: 1] [**] Pass [**]
 UTD WebFilter Whitelist [**] [URL: www.espn.go.com/m]
[VRF: vrf101] {TCP} 111.0.0.254:53511 -> 199.181.133.61:80
```

**ステップ 11** **show logging** | **include** CONFIG_DOWNLOAD

（オプション）ポリシー設定が適用されているかどうかを確認するログメッセージを表示します。次のようなメッセージを検索します。

..UTD MT 設定のダウンロードが開始されました（..UTD MT configuration download has started）

..UTD MT 設定のダウンロードが完了しました（..UTD MT configuration download has completed）

メッセージ ダウンロードが完了しました（download has completed）は、ポリシー設定が適用されたことを示します。

**例**：

```
show# logging | include CONFIG_DOWNLOAD
Aug 23 11:34:21.250 PDT: %IOSXE_UTD-4-MT_CONFIG_DOWNLOAD: UTD MT configuration download has started
Aug 23 11:54:18.496 PDT: %IOSXE_UTD-4-MT_CONFIG_DOWNLOAD: UTD MT configuration download has
completed
```

**ステップ 12** **show utd threat-inspection whitelist** [**profile** *profile-name*]

すべての許可リストのプロファイルまたは特定の許可リストのプロファイルを表示します。

**例**：

```
Device# show utd threat-inspection whitelist
Whitelist Profile: wh101
Signature ID: 101
```

**例**：

```
Device# show utd threat-inspection whitelist profile wh101
Whitelist Profile: wh101
Signature ID: 101
```

**ステップ 13** **show utd threat-inspection profile** *profile-name*

プロファイル名で指定された脅威検知プロファイルの詳細を表示します。

**例**：

```
Device# show utd threat-inspection profile 101
Threat-inspection Profile: 101
Operational Mode: Intrusion Protection
Operational Policy: Security
Logging Level: debug
Whitelist Profile: wh101
```

**ステップ 14** **show utd** [**policy** *profile-name*]

すべての UTD ポリシーまたは特定の UTD ポリシーを表示します。

**例**：

```
Device# show utd policy pol101
Policy name: pol101
VRF name: vrf101, VRF ID: 1
Global Inspection (across above VRFs): Enabled
Threat-inspection profile: 101
Web-filter URL profile: 1
Fail Policy: Fail-open
```

**ステップ 15** **show utd web-filter url** [**profile** *profile-name*]

すべての URL プロファイルまたは特定のプロファイルを表示します。

**例**：

```
Device# show utd web-filter url profile 1
URL Profile: 1
Alert: all
Blacklist Parameter Map Regex: urlf-blacklist1
Whitelist Parameter Map Regex: urlf-whitelist1
Block Categories:
dating
sports
Block Page Profile 1
Log level error
reputation block-threshold high-risk
```

**ステップ 16** **show utd web-filter block local-server** [**profile** *profile-name*]

すべてのブロックページのプロファイルまたは特定のブロックページのプロファイルを表示します。

**例**：

```
Device# show utd web-filter block local-server profile 2
Block Local Server Profile: 2
Content text: "Blocked by Web-Filter"
HTTP ports: 80
```

**ステップ 17** **show utd web-filter sourcedb** [**profile** *profile-name*]

すべての sourcedb プロファイルまたは特定の sourcedb プロファイルを表示します。

**例**：

```
Device# show utd web-filter sourcedb
SourceDB Profile: 1
database update server interval hour 0 minute 0
Fail open
Log level: error
Proxy host port 0

SourceDB Profile: 2
database update server interval hour 0 minute 0
Fail open
Log level: error
```

```
Proxy host port 0
```

例：

```
Device# show utd web-filter sourcedb profile 1
SourceDB Profile: 1
database update server interval hour 0 minute 0
Fail open
Log level: error
Proxy host port 0
```

**ステップ 18** **show utd engine standard statistics daq dp** [**engine** *engine-num*] [**vrf** [**name** *vrf-name* | **global**]]

すべての VRF または特定の VRF のサービスプレーンのデータ収集（DAQ：Data Acquistion）の統計情報を表示します。

例：

次の例は、VRF vrf101 のサービスプレーンのデータ収集の統計情報を示しています。

```
Device# show utd engine standard statistics daq dp vrf name vrf101
IOS-XE DAQ Counters(Engine #1):
--------------------------------
Frames received 374509
Bytes received 303136342
RX frames released 374509
Packets after vPath decap 374509
Bytes after vPath decap 284405526
Packets before vPath encap 372883
Bytes before vPath encap 283234522
Frames transmitted 372883
Bytes transmitted 300202270

Memory allocation 781856
Memory free 749636
Memory free via timer 29420
Merged packet buffer allocation 0
Merged packet buffer free 0

VPL buffer allocation 0
VPL buffer free 0
VPL buffer expand 0
VPL buffer merge 0
VPL buffer split 0
VPL packet incomplete 0

VPL API error 0
CFT API error 0
Internal error 52
External error 0
Memory error 0
Timer error 0

Kernel frames received 373590
Kernel frames dropped 0

FO cached via timer 0
Cached fo used 0
Cached fo freed 0
FO not found 0
CFT full packets 0
```

**ステップ 19** **show utd engine standard config threat-inspection whitelist** [**profile** *profile-name* ]

コンテナに保存されている脅威検知許可リストのプロファイルの詳細を表示します。

**例**：

```
Device# show utd engine standard config threat-inspection whitelist
UTD Engine Standard Configuration:

UTD threat-inspection whitelist profile table entries:
Whitelist profile: wh101
Entries: 1
```

**ステップ 20** **show utd engine standard config web-filter url profile** *profile-name*

コンテナに保存されている Web フィルタのプロファイルの詳細を表示します。

**例**：

```
Device# show utd engine standard config web-filter url profile 1
UTD Engine Standard Configuration:

UTD web-filter profile table entries
Web-filter URL profile: 1
Whitelist:
www.espn.com
www.nbcsports.com
www.nfl.com
Blacklist:
www.cnn.com
Categories Action: Block
Categories:
Social Network
Sports
Block Profile: 1
Redirect URL: http://172.27.56.97/vrf101.html
Reputation Block Threshold: High risk
Alerts Enabled: Whitelist, Blacklist, Categories, Reputation
Debug level: Error
Conditional debug level: Error
```

**ステップ 21** **show utd engine standard config** [**vrf name** *vrf-name* ]

特定の VRF に関連付けられた UTD ポリシー、脅威検知プロファイル、および Web フィルタプロファイルの詳細を表示します。

**例**：

```
Device# show utd engine standard config vrf name vrf101
UTD Engine Standard Configuration:

UTD VRF table entries:
VRF: vrf101 (1)
Policy: pol101
Threat Profile: 101
Webfilter Profile: 1
```

**ステップ 22** **show utd engine standard config threat-inspection profile** *profile-name*

特定の脅威検知プロファイルの詳細を表示します。

例：

```
Device# show utd engine standard config threat-inspection profile 101
UTD Engine Standard Configuration:

UTD threat-inspection profile table entries:
Threat profile: 101
Mode: Intrusion Prevention
Policy: Security
Logging level: Debug
Whitelist profile: wh101

Description:
Displays the details of a threat-inspection profile stored in the container.
```

**ステップ 23** **show utd engine standard threat-inspection signature update status**

現在の署名パッケージのバージョン、以前の署名パッケージのバージョン、および最後のステータス更新の出力を表示します。

例：

```
Device# show utd engine standard threat-inspection signature update status
Current signature package version: 29.0.c
Current signature package name: default
Previous signature package version: None
----------------------------------------
Last update status: Failed
----------------------------------------
Last successful update time: None
Last successful update method: None
Last successful update server: None
Last successful update speed: None
----------------------------------------
Last failed update time: Thu Jan 11 13:34:36 2018 PST
Last failed update method: Manual
Last failed update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
Last failed update reason: [Errno 113] No route to host
----------------------------------------
Last attempted update time: Thu Jan 11 13:34:36 2018 PST
Last attempted update method: Manual
Last attempted update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
----------------------------------------
Total num of updates successful: 0
Num of attempts successful: 0
Num of attempts failed: 1
Total num of attempts: 1
----------------------------------------
Next update scheduled at: None
----------------------------------------
Current status: Idle
```

**ステップ 24** **show platform software qfp active feature utd config [ vrf[ {id** *vrf-id* | **name** *vrf-name* | **global** } ]

サービスノードの統計情報を表示します。VRF情報は、マルチテナントの場合にのみ表示できます。データプレーンUTD設定を表示します。次の例では、セキュリティコンテキスト情報が強調表示されています。

例：

```
Device# Global configuration
  NAT64: disabled
```

```
SN threads: 12
CFT inst_id 0 feat id 0 fo id 0 chunk id 4
Context Id: 0, Name: Base Security Ctx
 Ctx Flags: (0xf0000)
      Engine: Standard
      SN Redirect Mode : Fail-close, Divert
      Threat-inspection: Enabled, Mode: IPS
      Domain Filtering : Not Enabled
      URL Filtering    : Not Enabled
 SN Health: Green
```

**ステップ 25** **show platform software utd interfaces**

例：

```
Device# show platform software utd interfaces

UTD interfaces
All dataplane interfaces
```

**ステップ 26** **show platform hardware qfp active feature utd config** [**vrf** {**id** *vrf-id* | **name** *vrf-name* | **global** } ]

UTD データパスの設定とステータスを表示します。

例：

```
Device# show platform hardware qfp active feature utd config vrf name vrf101
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  SN threads: 12
  CFT inst_id 0 feat id 1 fo id 1 chunk id 8
  SN Health: Green
```

**ステップ 27** **show platform hardware qfp active feature utd stats** [**clear** | **divert** | **drop** | **general** | **summary**] [**vrf** {**id** *vrf-id* | **name** *vrf-name* | **global** }] [all] [**verbose**]

ゼロのカウントを含むデータプレーン UTD 統計情報を表示します。

clear：統計情報をクリアします

divert：AppNav リダイレクト統計情報を表示します

drop：ドロップ統計情報を表示します

general：一般統計情報を表示します

summary：サマリー統計情報を表示します

verbose：Verbose 統計情報を表示します

VRF 統計情報ごとの VRF 表示：VRF 情報は、マルチテナントが有効な場合にのみ入力できます。

id：VRF ID に関連付けられた統計情報を表示します

name：指定した名前の VRF に関連付けられた統計情報を表示します

global：グローバル VRF（つまり VRF ID が 0）に関連付けられている統計情報を表示します

例：

```
Device# show platform hardware qfp active feature utd stats

Summary Statistics:
TCP Connections Created 29893
UDP Connections Created 24402
ICMP Connections Created 796
Pkts dropped pkt 258
byt 66365
Pkts entered policy feature pkt 715602
byt 562095214
Pkts entered divert feature pkt 662014
byt 516226302
Pkts slow path pkt 55091
byt 4347864
Pkts Diverted pkt 662014
byt 516226302
Pkts Re-injected pkt 659094
byt 514305557

Would-Drop Statistics:

Service Node flagged flow for dropping 258

General Statistics:
Non Diverted Pkts to/from divert interface 1022186
Inspection skipped - UTD policy not applicable 1081563

<output removed for brevity>
```

例：

**ステップ 28** **show platform hardware qfp active feature utd stats summary** [**vrf name** *vrf-name* | **all**]

**show platform hardware qfp active feature utd stats** コマンドのサマリーオプションから取得したすべての VRF または特定の VRF に関する情報を表示します。

例：

```
Device# show platform hardware qfp active feature utd stats vrf name vrf101
Security Context: Id:1 Name: 1 : vrf101

Summary Statistics:
TCP Connections Created 18428
UDP Connections Created 13737
ICMP Connections Created 503
Pkts dropped pkt 258
byt 66365
Pkts entered policy feature pkt 407148
byt 296496913
Pkts entered divert feature pkt 383176
byt 283158966
Pkts slow path pkt 32668
byt 2571632
Pkts Diverted pkt 383176
byt 283158966
Pkts Re-injected pkt 381016
byt 281761395
```

```
<output removed for brevity>
```

**ステップ 29** **show platform hardware qfp active feature utd stats drop all**

**show platform** コマンドのドロップオプションから取得したすべての VRF からの情報を表示します。

例：

```
Device# show platform hardware qfp active feature utd stats drop all

Would-Drop Statistics:

No diversion interface                                          0
No egress interface                                             0
Inspection service down                                         0
Could not find divert interface                                 0
Could not find divert fib                                       0
UTD FIB did not contain oce_chain                               0
Invalid IP version                                              0
IPS not supported                                               0
Re-inject Error                                                 0
Service Node flagged flow for dropping                       1225
Could not attach feature object                                 0
Could not allocate feature object                               0
Error getting feature object                                    0
Policy: could not create connection                             0
NAT64 Interface Look up Failed                                  0
Decaps: VPATH connection establishment error                    0
Decaps: VPATH could not find flow, no tuple                     0
Decaps: VPATH notification event error                          0
Decaps: Could not delete flow                                   0
Decaps: VPATH connection classification error                   0
Encaps: Error retrieving feature object                         0
Encaps: Flow not classified                                     0
Encaps: VPATH connection specification error                    0
Encaps: VPATH First packet meta-data failed                     0
Encaps: VPATH No memory for meta-data                           0
Encaps: VPATH Could not add TLV                                 0
Encaps: VPATH Could not fit TLV into memory                     0
Service Node Divert Failed                                      0
No feature object                                               0
Service Node not healthy                                      123
Could not allocate VRF meta-data                                0
Could not allocate debug meta-data                              0
Packet was virtually fragmented (VFR)                           0
IPv6 Fragment                                                   0
IPv4 Fragment                                                   0
```

# 統合脅威防御（UTD）のマルチテナントに関するトラブルシューティング

## トラフィックが転送されない

**問題** トラフィックは転送されません。

**考えられる原因** 仮想サービスがアクティブになっていない可能性があります。

**解決法** **show virtual-service list** コマンドを使用して、仮想サービスがアクティブになっているかどうかを確認します。次に、コマンドの出力例を示します。

```
Device# show virtual-service list

Virtual Service List:


Name Status Package Name
--------------------------------------------------------------------------------
snort Activated utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
```

**考えられる原因** 指定されたインターフェイスでは、統合脅威防御（UTD）が有効になっていない可能性があります。

**解決法** **show platform software utd global** コマンドを使用して、インターフェイスで UTD が有効になっているかどうかを確認します。

```
Device# show platform software utd global

UTD Global state
Engine               : Standard
Global Inspection    : Disabled
Operational Mode     : Intrusion Prevention
Fail Policy          : Fail-open
Container techonlogy : LXC
Redirect interface   : VirtualPortGroup1
UTD interfaces
GigabitEthernet0/0/0
```

**考えられる原因** サービスノードが正常に動作していない可能性があります。

**解決法** **show platform hardware qfp active feature utd config** コマンドを使用して、サービスノードの状態が緑色かどうかを確認します。

```
Device# show platform hardware qfp active feature utd config

Global configuration
NAT64: disabled
SN threads: 12
CFT inst_id 0 feat id 0 fo id 0 chunk id 4
Context Id: 0, Name: Base Security Ctx
Ctx Flags: (0x60000)
Engine: Standard
SN Redirect Mode : Fail-open, Divert
Threat-inspection: Enabled, Mode: IDS
Domain Filtering : Not Enabled
URL Filtering : Not Enabled
SN Health: Green
```

**解決法** また、マルチテナントの場合は、**show platform hardware qfp active feature utd config vrf name** *vrf-name*コマンドを使用して、特定の VRF 関するサービスノードの正常性が緑色であるかどうかを確認できます。

```
Device# show platform hardware qfp active feature utd config vrf name vrf102
Global configuration
  NAT64: disabled
  Drop pkts: disabled
```

```
  Multi-tenancy: enabled
  Data plane initialized: yes
  SN threads: 12
  CFT inst_id 0 feat id 0 fo id 0 chunk id 4
  SN Health: Green
```

**考えられる原因** Snort プロセスがアクティブになっていない可能性があります。

**解決法** **show virtual-service detail** コマンドを使用して、Snortプロセス が稼働しているかどうかを確認します。

```
Device# show virtual-service detail

Virtual service UTDIPS detail
  State                : Activated
  Owner                : IOSd
  Package information
    Name               : utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Path               : bootflash:/utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Application
      Name             : UTD-Snort-Feature
      Installed version : 1.0.1_SV2982_XE_16_3
      Description      : Unified Threat Defense
    Signing
      Key type         : Cisco development key
      Method           : SHA-1
    Licensing
      Name             : Not Available
      Version          : Not Available

  Detailed guest status

------------------------------------------------------------------------
Process               Status            Uptime           # of restarts
------------------------------------------------------------------------
climgr                 UP         0Y 0W 0D  0: 0:35        1
logger                 UP         0Y 0W 0D  0: 0: 4        0
snort_1                UP         0Y 0W 0D  0: 0: 4        0
Network stats:
eth0: RX  packets:43, TX  packets:6
eth1: RX  packets:8, TX  packets:6

Coredump file(s): lost+found

  Activated profile name: None
  Resource reservation
    Disk               : 736 MB
    Memory             : 1024 MB
    CPU                : 25% system CPU

  Attached devices
    Type              Name        Alias
    ---------------------------------------------
    NIC               ieobc_1     ieobc
    NIC               dp_1_0      net2
    NIC               dp_1_1      net3
    NIC               mgmt_1      mgmt
    Disk              _rootfs
    Disk              /opt/var
    Disk              /opt/var/c
    Serial/shell                  serial0
    Serial/aux                    serial1
    Serial/Syslog                 serial2
    Serial/Trace                  serial3
```

```
    Watchdog          watchdog-2

  Network interfaces
    MAC address             Attached to interface
    ------------------------------------------------------
    54:0E:00:0B:0C:02       ieobc_1
    A4:4C:11:9E:13:8D       VirtualPortGroup0
    A4:4C:11:9E:13:8C       VirtualPortGroup1
    A4:4C:11:9E:13:8B       mgmt_1

  Guest interface
  ---
  Interface: eth2
  ip address: 48.0.0.2/24
Interface: eth1
  ip address: 47.0.0.2/24

  ---

  Guest routes
  ---
  Address/Mask                          Next Hop                          Intf.
-------------------------------------------------------------------------------
0.0.0.0/0                             48.0.0.1                          eth2
0.0.0.0/0                             47.0.0.1                          eth1

  ---

  Resource admission (without profile) : passed
    Disk space    : 710MB
    Memory        : 1024MB
    CPU           : 25% system CPU
    VCPUs         : Not specified
```

**考えられる原因** AppNav トンネルがアクティブになっていない可能性があります。

**解決法** **show service-insertion type utd service-node-group** および **show service-insertion type utd service-context** コマンドを使用して、AppNav トンネルがアクティブになっているかどうかを確認します。

**解決法** 次に、**show service-insertion type utd service-node-group** コマンドの出力例を示します。

```
Device# show service-insertion type utd service-node-group

Service Node Group name : utd_sng_1
Service Context : utd/1
Member Service Node count : 1


Service Node (SN) : 30.30.30.2
Auto discovered : No
SN belongs to SNG : utd_sng_1
Current status of SN : Alive
Time current status was reached : Tue Jul 26 11:57:48 2016

Cluster protocol VPATH version : 1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1469514497
Cluster protocol last received sequence number: 1464
Cluster protocol last received ack number : 1469514496
```

**解決法** 次に、**show service-insertion type utd service-context** コマンドの出力例を示します。

```
Device# show service-insertion type utd service-context

Service Context : utd/1
Cluster protocol VPATH version : 1
Time service context was enabled : Tue Jul 26 11:57:47 2016
Current FSM state : Operational
Time FSM entered current state : Tue Jul 26 11:57:58 2016
Last FSM state : Converging
Time FSM entered last state : Tue Jul 26 11:57:47 2016
Cluster operational state : Operational

Stable AppNav controller View:
30.30.30.1

Stable SN View:
30.30.30.2

Current AppNav Controller View:
30.30.30.1

Current SN View:
30.30.30.2
```

**考えられる原因** トラフィックのステータスのデータプレーンUTD統計情報を確認します。トラフィックが転送されない場合、転送および拒否されたパケットの数はゼロになります。数値がゼロ以外の場合、トラフィック転送が行われており、Snort センサーはデータプレーンにパケットを再送信しています。

**解決法** **show platform hardware qfp active feature utd stats** コマンドを使用してトラフィックのステータスを確認します。

```
Device# show platform hardware qfp active feature utd stats

Security Context:    Id:0    Name: Base Security Ctx

Summary Statistics:
Active Connections                                                  29
TCP Connections Created                                         712910
UDP Connections Created                                             80
Pkts entered policy feature                         pkt       3537977
                                                    byt     273232057
Pkts entered divert feature                         pkt       3229148
                                                    byt     249344841
Pkts slow path                                      pkt        712990
                                                    byt      45391747
Pkts Diverted                                       pkt       3224752
                                                    byt     249103697
Pkts Re-injected                                    pkt       3224746
                                                    byt     249103373
….
```

**解決法** また、マルチテナントの場合は、**show platform hardware qfp active feature utd stats vrf name** *vrf-name*コマンドを使用して、特定の VRF に関するトラフィックのステータスを確認できます。

```
Device# show platform hardware qfp active feature utd stats vrf name vrf 101

Security Context:    Id:1    Name: 1 : vrf101

Summary Statistics:
Active Connections                                                      2
TCP Connections Created                                             34032
UDP Connections Created                                             11448
ICMP Connections Created                                               80
Pkts dropped                                          pkt             626
                                                      byt          323842
Pkts entered policy feature                           pkt          995312
                                                      byt       813163885
Pkts entered divert feature                           pkt          639349
                                                      byt       420083106
Pkts slow path                                        pkt           45560
                                                      byt         7103132
Pkts Diverted                                         pkt          638841
                                                      byt       419901335
Pkts Re-injected                                      pkt          630642
                                                      byt       412139098
….
```

# 署名の更新が機能しない

**問題**　Cisco ボーダレスソフトウェア配布（BSD：Borderless Software Distribution）サーバからの署名更新が機能していません。

**考えられる原因**　さまざまな理由により署名の更新に失敗した可能性があります。最後に署名の更新に失敗した理由を確認します。

**解決法**　**show utd engine standard threat-inspection signature update status** コマンドを使用して、最後に署名の更新に失敗した理由を表示します。

```
Device# show utd eng standard threat-inspection signature update status
Current signature package version: 29.0.c
Current signature package name: default
Previous signature package version: None
----------------------------------------
Last update status: Failed
----------------------------------------
Last successful update time: None
Last successful update method: None
Last successful update server: None
Last successful update speed: None
----------------------------------------
Last failed update time: Thu Jan 11 13:34:36 2018 PST
Last failed update method: Manual
Last failed update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
Last failed update reason: [Errno 113] No route to host
----------------------------------------
Last attempted update time: Thu Jan 11 13:34:36 2018 PST
Last attempted update method: Manual
Last attempted update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
----------------------------------------
Total num of updates successful: 0
Num of attempts successful: 0
Num of attempts failed: 1
```

```
Total num of attempts: 1
----------------------------------------
Next update scheduled at: None
----------------------------------------
Current status: Idle
```

**考えられる原因** ドメインネームシステム（DNS）が正しく設定されていません。

**解決法** **show running-config | i name-server** コマンドを使用して、ネームサーバの詳細を表示します。

```
Device#  show run | i name-server

ip name-server 10.104.49.223
```

**考えられる原因** システムエラー：ユーザ名とパスワードの組み合わせの処理に失敗しました。

**解決法** 署名パッケージのダウンロードに正しい認証情報を使用したことを確認します。

# ローカルサーバからの署名の更新が機能しない

**問題** ローカルサーバからの署名の更新が機能しない。

**考えられる原因** 最後の失敗の理由：無効なスキーム — HTTP または HTTPS のみに対応します。

**解決法** ローカルダウンロード方式として HTTP またはセキュア HTTP（HTTPS）が指定されていることを確認します。

**考えられる原因** 最後の失敗の理由：名前またはサービスが不明です。

**解決法** ローカルサーバに指定されたホスト名または IP アドレスが正しいことを確認します。

**考えられる原因** 最後の失敗の理由：認証情報が入力されていません。

**解決法** ローカル HTTP または HTTPS サーバの認証情報が入力されていることを確認します。

**考えられる原因** 最後の失敗の理由：ファイルが見つかりません。

**解決法** 入力した署名ファイル名または URL が正しいことを確認します。

**考えられる原因** 最後の失敗の理由：ダウンロードが破損しています。

**解決法**

- 以前の署名のダウンロード時に署名更新の再試行でエラーが発生していないかどうかを確認します。
- 正しい署名パッケージが使用可能であることを確認します。

# IOSd Syslog へのロギングが機能しない

**問題** IOSd syslog へのロギングが機能しない。

**考えられる原因** syslog へのロギングは、統合脅威防御（UTD）の設定では設定できません。

**解決法** UTD 設定を表示し、syslog へのロギングが設定されていることを確認するには、**show utd engine standard config** コマンドを使用します。

```
Device# show utd engine standard config

UTD Engine Standard Configutation:
  Operation Mode : Intrusion Prevention
  Policy         : Security

Signature Update:
  Server    : cisco
  User Name : ccouser
  Password  : YEX^SH\fhdOeEGaOBIQAIcOVLgaVGf
  Occurs-at : weekly ;  Days:0 ; Hour: 23; Minute: 50

Logging:
  Server    :   IOS Syslog; 10.104.49.223
  Level     : debug

Whitelist Signature IDs:
  28878
```

**解決法** UTD エンジンのイベントログを表示するには、次の **show utd engine standard logging events** コマンドを使用します。

```
Device# show utd engine standard logging events

2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected]
[Priority: 1] [VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53
2016/06/13-14:32:21.524988 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} a000:0:0:0:0:0:0:10:59964 -> b000:0:0:0:0:0:0:10:53
```

# 外部サーバへのロギングが機能しない

**問題** 外部サーバへのロギングが機能していません。

**考えられる原因** 外部サーバで Syslog が実行されていない可能性があります。

**解決法** syslog サーバが外部サーバで実行されているかどうかを確認します。ステータスを表示するには、外部サーバで次のコマンドを設定します。

```
ps -eaf | grep syslog

 root 2073 1 0 Apr12 ? 00:00:02 syslogd -r -m
```

**考えられる原因**　統合脅威防御（UTD）の Linux コンテナ（LXC：Linux Container）と外部サーバ間の接続が失われている可能性があります。

**解決法**　管理インターフェイスから外部 syslog サーバへの接続を確認します。

# UTD 条件付きデバッグ

条件付きデバッグは、Unified Threat Defense のマルチテナントに対応しています。条件付きデバッグの設定方法の詳細については、以下を参照してください。

http://www.cisco.com/c/en/us/td/docs/routers/asr1000/troubleshooting/guide/Tbl-shooting-xe-3-asr-1000-book.html#task_AC969BB06B414DCBBDEF7ADD29EF8131