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 （9 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 （11 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。

（注） 許可またはブロック正規表現パターンで *www* プレフィックスを使用している場合、クライアントメッセージで返されるサーバー名インジケータ（SNI）が一致しない場合に問題が発生する可能性があります。たとえば、*www./foo./com* を許可する場合、SNI は *foo.com* としてのみ返されます。正規表現による照合には *www* を含めないことをお勧めします。

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

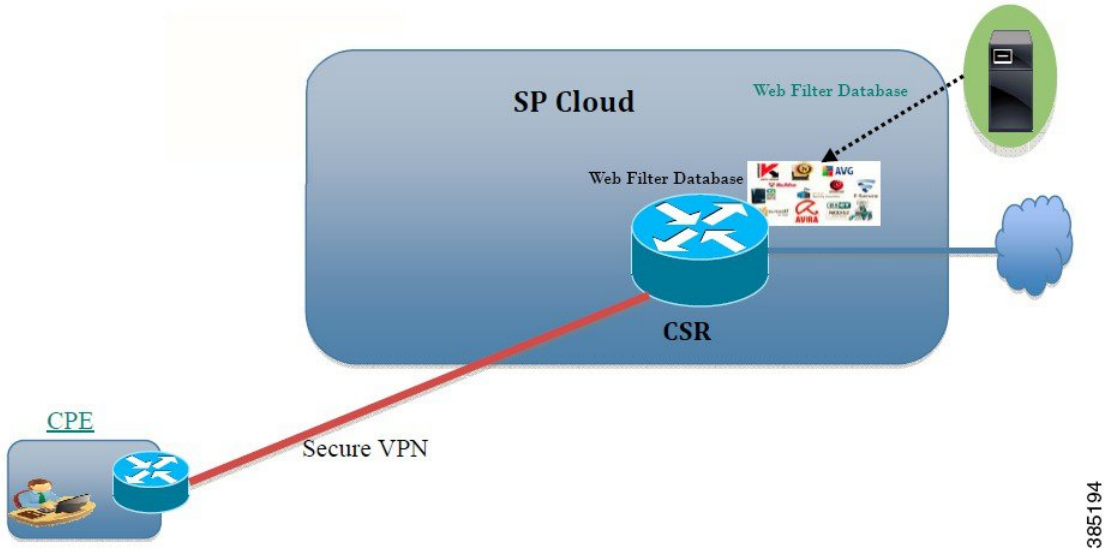
ンの検索は、URL のホスト部分にドメイン名がある場合にのみ実行されます。完全なデータベースがクラウドからダウンロードされた後、既存のデータベースに更新がある場合、差分の更新が 15 分ごとに自動的にダウンロードされます。完全なデータベースのサイズは約 440 MB で、ダウンロードしたデータベースは常にクラウドと同期する必要があります。クラウドへの接続が 24 時間以上失われると、データベースは無効になります。

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 *1 : 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。そのような URL を許可するには、それらを許可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 （8 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 （9 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 （11 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 （12 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 （15 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 （16 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 （8 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 （9 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 （9 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 （9 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 （9 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 （9 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**
- **show utd engine standard logging events**

（注） このツールは、設定された URL フィルタリングアラート/イベントの出力のみを表示します。ユーザーは、「設定例」セクションの手順に従って、この出力に表示されるイベントとアラートのタイプを設定できます。たとえば、「alert all」を設定した場合は、「ホワイトリスト」、「ブラックリスト」、およびカテゴリとレピュテーションのイベントが表示されます。「alert whitelist」のみを設定すると、「ホワイトリスト」イベントのみが表示されます。

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）。

次のサイト https://www.brightcloud.com/tools/url-ip-lookup.php を使用すると、URL フィルタリング機能によって Web サイトがどのように分類されるのかを検証できます。

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 の許可リスト署名の設定

次の例は、署名の許可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]
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』 [英語] • 『Cisco IOS Security Command Reference: Commands M to R』 [英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
UCS E シリーズ サーバ	http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/2-0/gs/guide/b_2_0_Ge

シスコのテクニカル サポート

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

Cisco 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 *1 : 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 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。 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。 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。 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。

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