Webセキュリティアプライアンスを設定する方法WebExアプリケーションの追加パススルー設定

はじめに

このドキュメントでは、特別な導入状況でCisco Webexアプリケーションの機能を適切に確保するために、セキュアWebアプライアンス(SWA/WSA)バイパスポリシーを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Async OS for Secure Web Appliance 14.x以降。
- Secure Web Appliance Graphic User Interface(GUI)への管理ユーザー・アクセス。
- Secure Web Applianceのコマンドラインインターフェイス(CLI)への管理ユーザアクセス。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

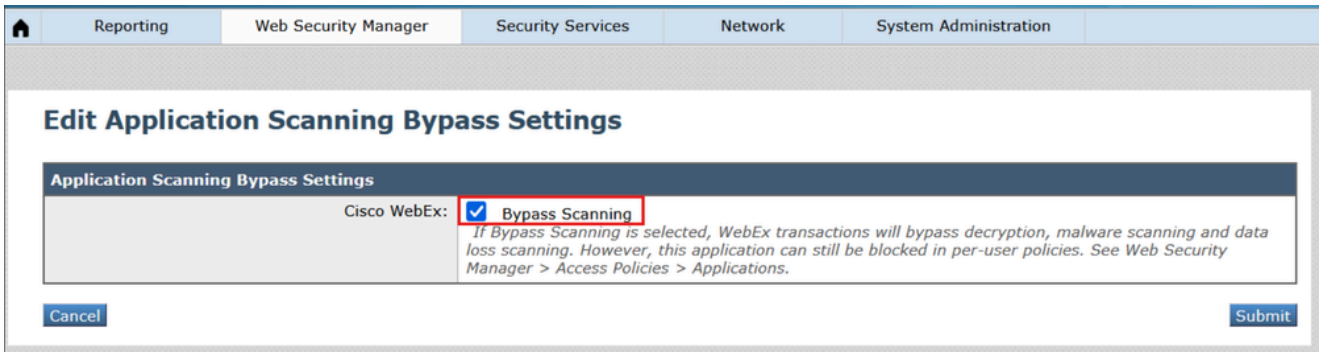
『Webexサービスのネットワーク要件』のWebexの公開文書に基づき、Webexシグナリングトラフィックがドキュメントに記載されているドメイン/URLにアクセスできるようにプロキシサーバを設定する必要があります。Secure Web Applianceは、バイパス設定でWebExアプリケーションバイパスチェックボックスを有効にすることによって、ほとんどの環境の要件を満たします。ただし、WebExアプリケーションのサービス中断を回避するために、Secure Web Applianceで追加の構成が必要になる場合があります。このような場合には、次の手順が推奨されます。

Webexアプリケーションスキャンバイパス

Cisco WebEx：スキャンのバイパス機能は、WebExアプリケーショントラフィックがフィルタリングされずにセキュアWebアプライアンスを通過できるようにする最初のステップです。WebExデスクトップアプリケーションまたはモバイルアプリケーションのユーザがWebトラフィックをSecure Web Appliance経由でプロキシされるすべての環境および導入シナリオで有効にする必要があります。

Webexアプリケーションスキャンバイパスを有効にする手順：

1. WSA GUIで、Web Security Manager > Bypass Settings > Edit Application Bypass Settingsの順に表示します。
2. 「Cisco WebEx」のチェックボックスをオンにします。



1_wsa_bypass_scanning_settings

3. 変更を送信して確定します。

この設定を有効にすると、FQDNがSecure Web Applianceのバイパスリストに追加された後に予想されるとおり、透過トラフィックはバイパスされません。むしろ、Webexアプリケーショントラフィックは引き続きセキュアWebアプライアンスを介してプロキシされますが、決定タグ「PASSTHRU_AVC」を使用して復号化に渡されます。 アクセスログの表示例を次に示します。

```
1761695285.658 55398 192.168.100.100 TCP_MISS/200 4046848 TCP_CONNECT 3.161.225.70:443 - DIRECT/binarie
```

固有の環境に関する考慮事項

トラフィックがセキュアWebアプライアンスを介してプロキシされるときにWebExアプリケーションが動作するように追加設定が必要になる、いくつかのシナリオがあります。

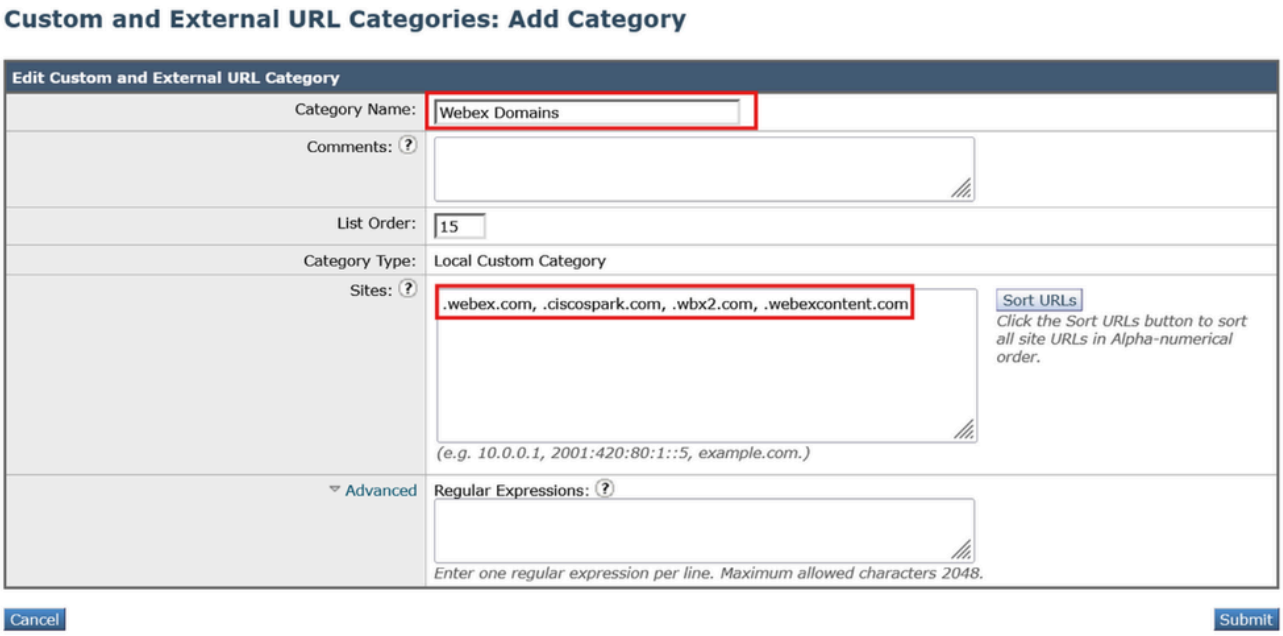
シナリオ1:Webexドメインを認証から除外する必要がある

これは、IPサロゲートが識別プロファイルで有効になっておらず、透過的なリダイレクションが使用されている環境で特に顕著です。既存のドキュメントに基づき、Webexアプリは、プロキシが明示的に定義されているドメインに参加しているワークステーション上でNTLMSSP認証を実行できます。それ以外の場合は、Webexドメインのカスタムカテゴリを設定し、認証から除外することがベストプラクティスです。

Webexドメインを認証から除外する手順：

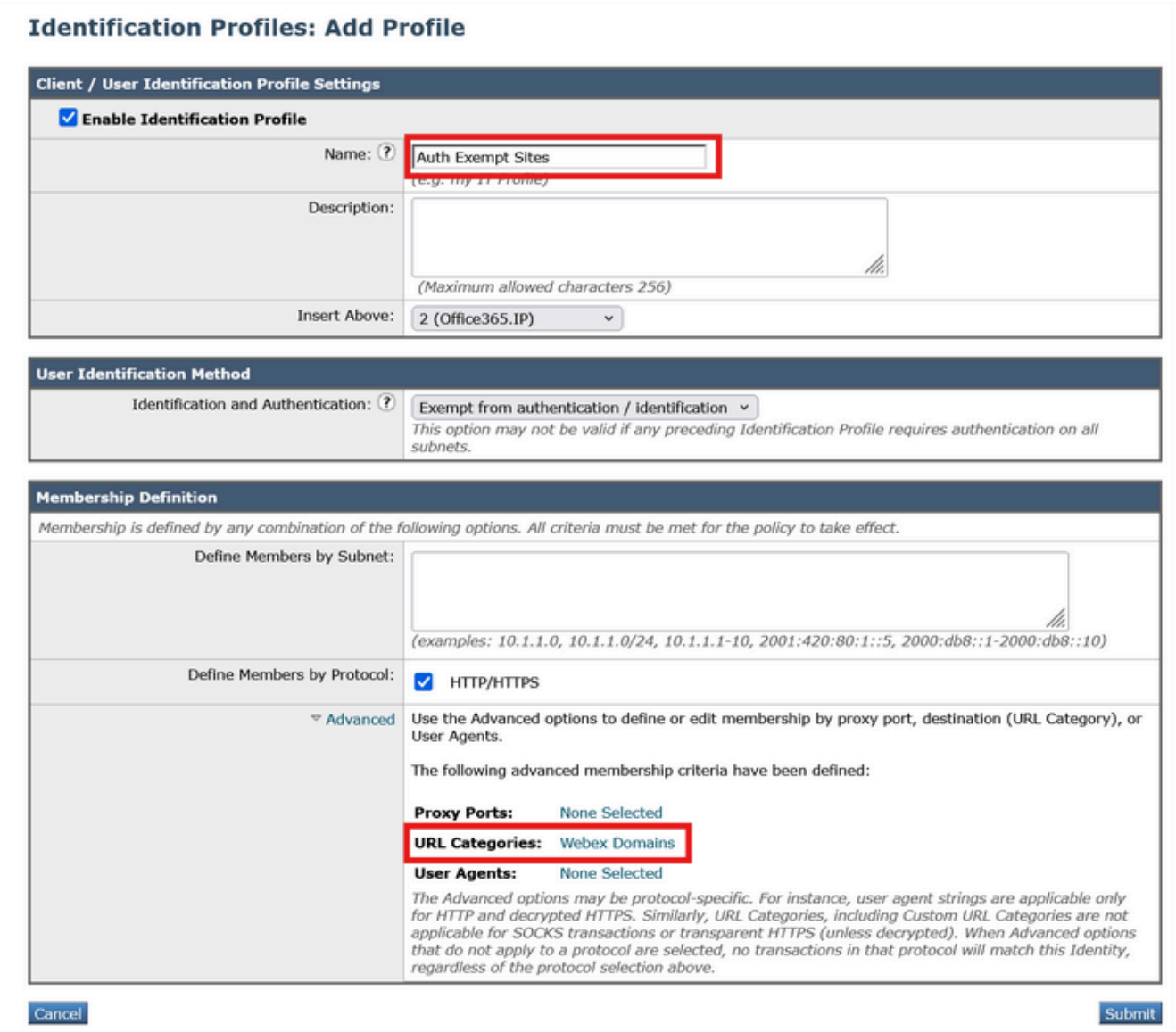
1. WSA GUIで、Web Security Manager > Custom and External URL Categories > Add Categoryの順に移動します。
2. 新しいカテゴリに名前を付け、次のドメインをSitesセクションに配置します。

```
.webex.com, .ciscospark.com, .wbx2.com, .webexcontent.com
```



2_wsa_custom_url_category

3. [Submit] をクリックします。次に、Web Security Manager > Identification Profiles > Add Identification Profileの順に移動します
4. 新しいプロファイルに名前を付け、URL CategoriesのAdvancedセクションで、ステップ#2で作成した新しいカテゴリを選択します



3_wsa_id_profile

5. 新しいプロファイルのIDと認証が認証/識別から除外されるように設定されていることを確認します。
6. 送信し、変更を確定します。

シナリオ2:Webexコンテンツドメインは復号化バイパスの対象とはなりません。

webexcontent.comに関連して、Webexアプリケーションスキャンバイパスが有効な場合に、復号時に自動的にパススルーされないサブドメインがいくつかあります。 これらのドメインから提供されるコンテンツは、Secure Web Applianceの復号化証明書がデバイスの信頼できるルート証明書ストアにすでに追加されている限り、またはWebexアプリを実行しているデバイスによってすでに信頼されている内部認証局によって署名されている限り、復号化される際にWebexアプリによって信頼されます。ただし、デバイスが管理されておらず、セキュアWebアプライアンスの復号化証明書が信頼されていない場合、これらのドメインは復号化時にパススルーするように設定する必要があります。

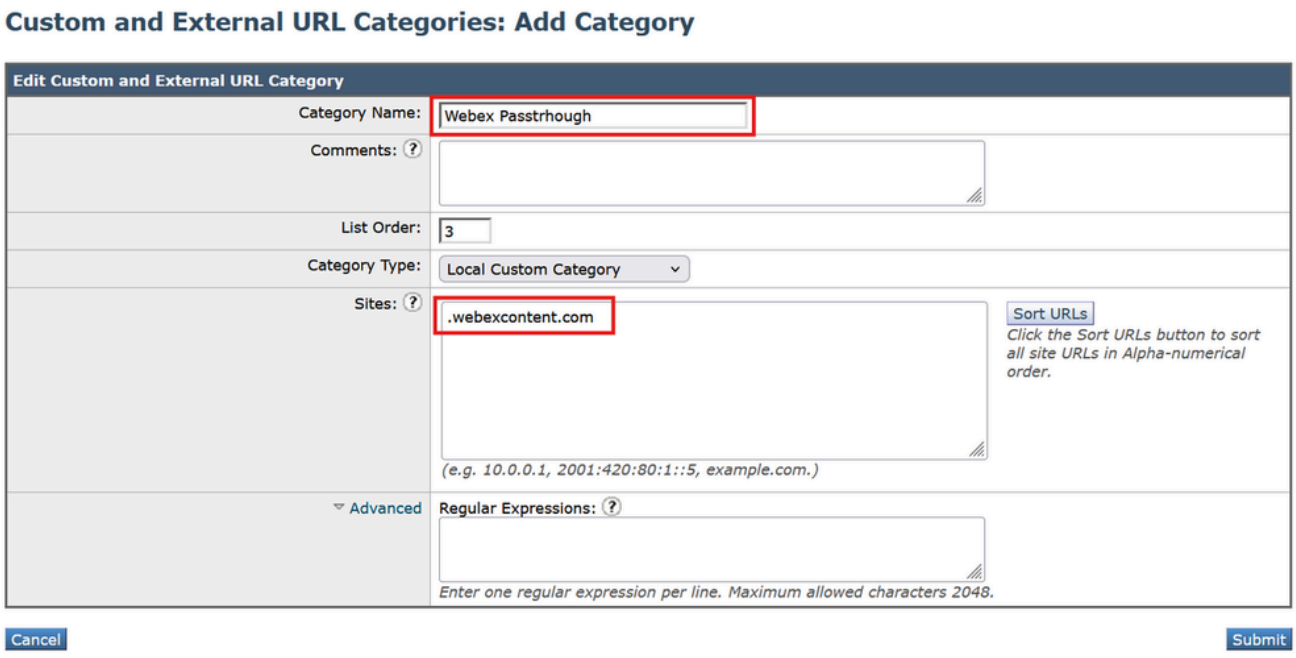
透過的なリダイレクション導入が行われており、リダイレクショングループに使用されるクライアントIPスプーフィングに沿って複数のSWAがある場合、トラフィックは宛先IPに基づいてセキ

ユアWebアプライアンスにリダイレクトするように設定でき、同様にWebサーバからのリターントラフィックは送信元アドレスに基づいてセキュアWebアプライアンスを介してリダイレクトして戻るように設定できます。セキュアWebアプライアンスが、DNSルックアップを使用して解決するIPを使用してWebサーバに接続するように設定されている場合、リターントラフィックが誤って別のセキュアWebアプライアンスにリダイレクトされ、その後ドロップされる可能性があります。この問題は、Webサーバで循環IPアドレスを使用するため、WebExだけでなく、他のビデオストリーミングアプリケーションにも影響を与えます。

すべてのWebexドメインの復号化でパススルーを設定する手順は次のとおりです。

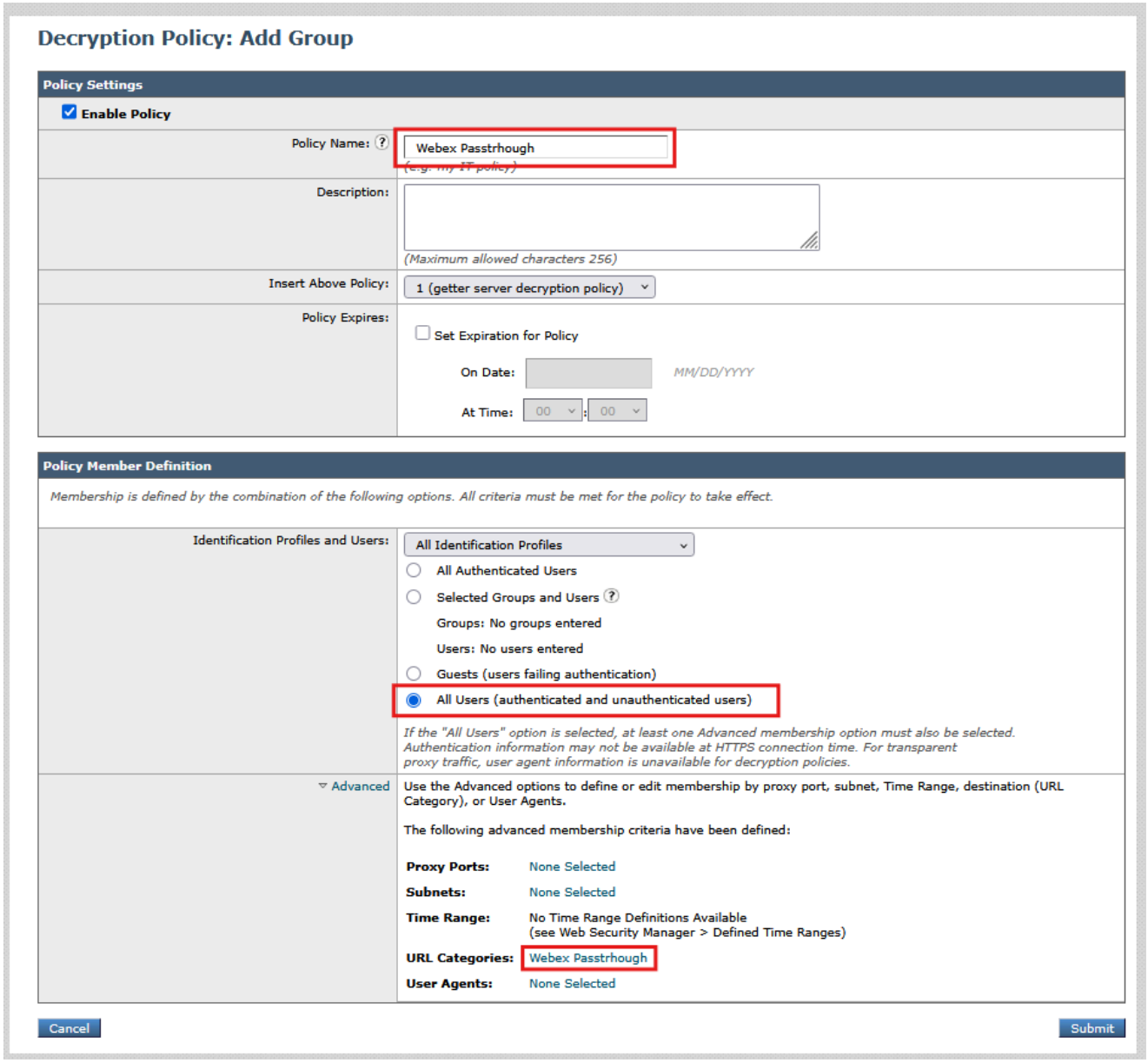
1. 上記の手順に従って、Webexアプリケーションスキャンバイパスが有効になっていることを確認します。
2. WSA GUIで、Web Security Manager > Custom and External URL Categories > Add Categoryの順に移動します。
3. 新しいカテゴリに名前を付け、次のドメインをSitesセクションに配置します。

```
.webexcontent.com
```



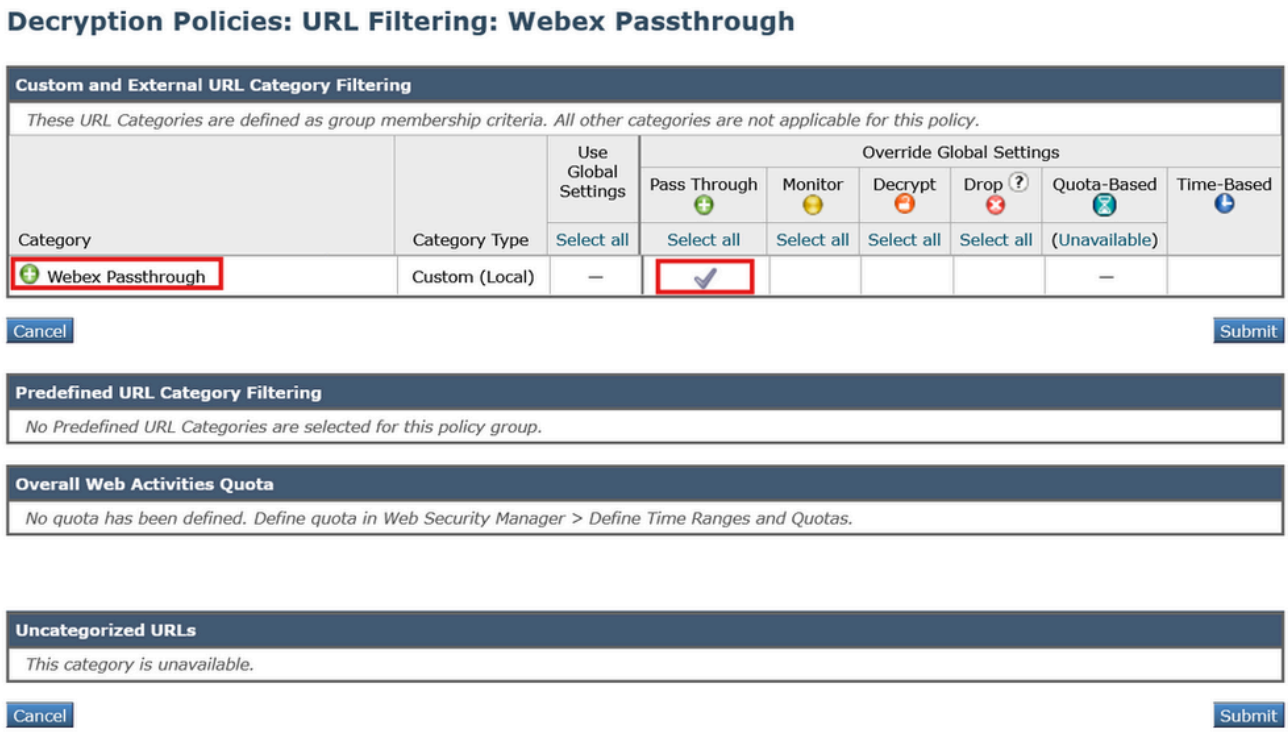
4_wsa_url_カテゴリ

4. [Submit] をクリックします。ここで、Web Security Manager > Decryption Policies > Add Policyの順に移動します
5. 新しいポリシーに名前を付け、Identification Profiles and UsersをAll Usersに設定し、URL CategoriesのAdvancedセクションでステップ#3で作成した新しいカテゴリを選択します



5_wsa_decryption_policy（復号化ポリシー）

6. [Submit] をクリックします。次に、URL Filteringセクションをクリックし、ステップ#3で作成したカスタムカテゴリをPass Throughに設定します。



6_wsa_url_フィルタリング

7. 変更を [Submit] して [Commit] します。

透過的なリダイレクションに複数のSecure Web Appliance(HTTPS)が導入されており、クライアントのIPスプーフィングが有効になっている場合は、この問題に対して2つの解決策があります。

1. 発信WCCPサービスとリターンWCCPサービスを、サーバアドレスではなくクライアントアドレスに基づいてロードバランスするように設定します。
2. WSA CLIで、advancedproxyconfig > DNS > Find web server byの順に設定し、Webサーバへの接続に対してクライアントが指定したIPアドレス（オプション2および3）を常に使用するようにします。 この設定の詳細については、『セキュアWebアプライアンスの使用のベストプラクティス』ガイドの「DNS」セクションを参照してください。

検証

パススルー設定が完了すると、Webexトラフィックはポリシーに従ってパススルーとしてアクセスログで処理されます。

```
1763752739.797 457 192.168.100.100 TCP_MISS/200 6939 TCP_CONNECT 135.84.171.165:443 - DIRECT/da3-wxt08-
1763752853.942 109739 192.168.100.100 TCP_MISS/200 7709 TCP_CONNECT 170.72.245.220:443 - DIRECT/avatar-
1763752862.299 109943 192.168.100.100 TCP_MISS/200 8757 TCP_CONNECT 18.225.2.59:443 - DIRECT/highlights
1763752870.293 109949 192.168.100.100 TCP_MISS/200 8392 TCP_CONNECT 170.72.245.190:443 - DIRECT/retenti
```

WebExアプリケーションをレビューして監視します。速度低下やサービス中断が報告された場合は、アクセスログをもう一度確認し、すべてのWebEx側トラフィックが正しく処理されていることを検証します。

関連情報

- Webexサービスのネットワーク要件
- セキュアなWebアプライアンスのベストプラクティスの使用

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。