

Secure Web Applianceでのアップストリームプロキシの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[アップストリームプロキシの設定](#)

[ステップ2: \(オプション\) アップストリームプロキシを使用するIDプロファイルの作成](#)

[ステップ3アップストリームプロキシの作成](#)

[ステップ4: \(オプション\) 復号化証明書をアップロードします。](#)

[ステップ5ルーティングポリシーの設定](#)

[ステップ6: \(オプション\) アップストリームプロキシ応答しないタイムアウト設定の設定](#)

[Logging](#)

[アクセスログ](#)

[Proxylogs](#)

[関連情報](#)

はじめに

このドキュメントでは、Secure Web Appliance(SWA)でアップストリームプロキシ(UPSTREAM PROXY)を設定する手順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。

- SWA管理。
- 基本的なネットワークングおよびプロキシプロトコル。

次のツールをインストールしておくことを推奨します。

- 物理または仮想SWA
- SWAグラフィカルユーザインターフェイス(GUI)への管理アクセス
- SWAコマンドラインインターフェイス(CLI)への管理アクセス


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たものです。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。

アップストリームプロキシの設定

SWAでアップストリームプロキシを設定するには、次の手順を使用します。


手順	手順
ステップ1: (オプション) URLに対するカスタムURLカテゴリの作成	ステップ1.1:GUIから、Web Security Managerを選択し、カスタムおよび外部URLカテゴリをクリックします。 ステップ1.2 : カテゴリの追加をクリックして、カスタムURLカテゴリを追加します。
 注 : すべてのトラフィックに対してアップストリームプロキシを定義する場合は、このステップを省略できます。	手順1.3:一意のCategoryNameを割り当てます。 ステップ1.4: (オプション) 説明を追加する。 ステップ 1.5 : リスト順から、一番上に配置する最初のカテゴリを選択します。 ステップ 1.6 : Category Typeドロップダウンリストから、Local Custom Categoryを選択します。 ステップ 1.7 : Sitesセクションに必要なURLを追加します。 ステップ 1.8 : [Submit] をクリックします。

Custom and External URL Categories: Add Category

The screenshot shows a web form titled "Edit Custom and External URL Category". The form has several fields: "Category Name" (containing "Use Upstream Proxy"), "Comments" (with a help icon), "List Order" (a dropdown menu set to "1"), "Category Type" (a dropdown menu set to "Local Custom Category"), "Sites" (containing "www.cisco.com, .cisco.com"), and "Regular Expressions" (with a help icon). A "Sort URLs" button is located to the right of the "Sites" field. At the bottom, there are "Cancel" and "Submit" buttons. Red circles with numbers 1.3 through 1.7 are overlaid on the form, with arrows pointing to the "Category Name", "List Order", "Category Type", "Sites", and "Regular Expressions" fields respectively.

イメージ - カスタムURLカテゴリの作成

ステップ2: (オプション) アップストリームプロキシを使用するIDプロファイルの作成

 注 : すべてのトラフィックに対してアップストリームプロキシを定義する場合は、このステップを省略できます。

ステップ2.1:GUIから、Web Security Managerを選択し、Identification Profilesをクリックします。
ステップ2.2 : プロファイルを追加するには、プロファイルの追加をクリックします。
ステップ2.3 : このプロファイルを有効にする、または削除せずにすばやく無効にするには、Enable Identification Profileチェックボックスを使用します。
手順2.4:一意のprofileNameを割り当てます。
ステップ2.5: (任意) 説明を追加する。
ステップ2.6:上記の挿入ドロップダウンリストから、このプロファイルをテーブルのどこに表示するかを選択する。
ステップ 2.7 : このポリシーに一致するユーザを認証しない場合は、「ユーザ識別方法」セクションで「認証/識別から免除」を選択するか、認証パラメータを設定します。
手順2.8:特定のIPアドレスのトラフィックをパススルーする場合を除き、このフィールドを空白のままにして、すべてのクライアントIPアドレスを含めます (デフォルトのIPアドレスは使用しない) 。
ステップ2.9.(オプション:特定のWebサイトにアクセスする特定のユーザに対してアップストリームプロキシを使用する必要がある場合は、このステップを実行します。)
Advancedセクションで、Custom URL Categoriesを選択し、ステップ1で作成したCustom URL Categoryを追加します
ステップ 2.10 : [Submit] をクリックします。

Identification Profiles: Add Profile

The screenshot shows the 'Client / User Identification Profile Settings' page. It is divided into three main sections: 'Client / User Identification Profile Settings', 'User Identification Method', and 'Membership Definition'. Red circles with numbers 2.4 through 2.9 point to specific fields in the interface.

- 2.4** points to the 'Name' field, which contains 'Upstream Proxy ID Profile'.
- 2.6** points to the 'Insert Above' dropdown menu, which is set to '1 (AD Group Test)'.
- 2.7** points to the 'Authentication Method' section, specifically the 'Authenticate Users' dropdown and the 'Select a Scheme' dropdown.
- 2.8** points to the 'Define Members by Subnet' field, which contains '10.0.0.0/8'.
- 2.9** points to the 'Advanced' options section, specifically the 'Proxy Ports', 'URL Categories', and 'User Agents' fields, all of which are set to 'None Selected'.

イメージ – 識別プロファイルの作成

ステップ 3 アップストリームプロキシの作成

ステップ 3.1: GUI から、Network を選択し、Upstream Proxy をクリックします。

ステップ 3.2 : [グループの追加] をクリックします。

ステップ 3.3: uniqueName を割り当てます。

ステップ 3.4 : プロキシアドレスとポート番号を定義します。

ステップ 3.5.(オプション) 複数のアップストリームプロキシがある場合は、Add Row をクリックして次のプロキシを定義します。

ステップ 3.6.(オプション) 「ロードバランシング」セクションから複数のアップストリームプロキシを入力した場合は、必要なロードバランシング方式を定義します。

- なし (フェールオーバー) : Web プロキシは、グループ内の 1 つの外部プロキシにトランザクションを転送します。プロキシは、リストされている順序で接続を試みます。1 つのプロキシに到達できない場合、Web プロキシはリスト内の次のプロキシへの接続を試みます。
- 接続が最も少ない: Web プロキシは、グループ内の異なるプロキシに対するアクティブな要求の数を追跡し、現在最も少ない接続にサービスを提供しているプロ

キシにトランザクションを転送します。

- ハッシュベース:最も最近の使用頻度が低い。Webプロキシは、すべてのプロキシが現在アクティブな場合、トランザクションを最近受信しなかったプロキシにトランザクションを転送します。この設定はラウンドロビンに似ていますが、Webプロキシは別のプロキシグループのメンバーであることによってプロキシが受信したトランザクションも考慮に入れる点が異なります。つまり、プロキシが複数のプロキシグループにリストされている場合、「least recently used」オプションがプロキシに過剰な負荷をかけることが少なくなります。
- ラウンドロビン:Webプロキシは、リストされた順序で、グループ内のすべてのプロキシ間でトランザクションを均等に循環させます。

ステップ 3.7 : 内部ポリシーに応じて、Failure Handlingオプションを選択します。

- 直接接続:要求を宛先サーバに直接送信します。
- ドロップ要求:転送せずに要求を破棄します。

ステップ 3.8 : [Submit] をクリックします。

Add Upstream Proxy Group


Proxy Address	Port	Reconnection Attempts (?)	Add Row
10.48.48.182	3128	2	<input type="button" value="Add Row"/>
10.48.48.183	3128	2	<input type="button" value="Add Row"/>

Load Balancing: Fewest Connections

Failure Handling: Connect directly Drop requests

イメージ : アップストリームプロキシグループの追加

ステップ4: (オプション) 復号化証明書をアップロードします。

 注 : アップストリームプロキシがトラフィックを復号していないか、またはそのCAサーバがすでにSWAで信頼されている場合は、このステップを省略できます

ステップ4.1:GUIから、Networkを選択し、Certificate Managementをクリックします。

ステップ 4.2 : Certificate Managementセクションで、Manage Trusted Root Certificatesをクリックします。

Certificate Management

Appliance Certificates

Add Certificate...

Certificate	Common Name	Issued By	Domains	Status	Time Remaining	Expiration Date	Delete
-------------	-------------	-----------	---------	--------	----------------	-----------------	--------

Export Certificate...

Weak Signature Usage Settings

Restrict Weak Signature Usage: Disabled [Edit Settings](#)

Certificate FQDN Validation Settings

Certificate FQDN Validation Usage: Disabled [Edit Settings](#)

Certificate Lists

Updates

File Type	Last Update	Current Version	New Update
Cisco Trusted Root Certificate Bundle	Success - Sat Mar 07 00:08:32 2026	2.6	Failed to Fetch Manifest
Cisco Certificate Blocked List	Success - Sat Mar 07 00:08:32 2026	1.3	Failed to Fetch Manifest

No updates in progress. [Update Now](#)

Certificate Management

Trust Root Certificates: 246 certificates in Cisco trusted root certificate list
0 custom certificates added to trusted root certificate list [Manage Trusted Root Certificates...](#)

Certificate Based Authentication/RADSEC Root Certificates: 0 custom root certificates added to Certificate Based Authentication/RADSEC root certificate list [Manage Certificate Based Authentication/RADSEC Root Certificates...](#)

Blocked Certificates: 19 certificates in Cisco blocked certificate list [View Blocked Certificates...](#)

イメージ - 信頼されたルート証明書の管理

ステップ 4.3 : 送信し、変更を確定します。

! 注意: ルートCA証明書と中間CA証明書の両方が必要な場合は、まずルートCA証明書をアップロードしてから、Submit and Commitをクリックします。コミットが完了したら、中間CA証明書をインポートし、変更を送信してコミットします。

ステップ 5 ルーティングポリシーの設定

ステップ 5.1 : GUIで、Web Security Managerを選択し、Routing Policyをクリックします。

ステップ 5.2. (オプション) 特定のユーザまたはWebサイトにアップストリームプロキシを使用する場合は、Add Policyをクリックし、ステップ 2 で作成したIDプロファイルを選択します。

Routing Policy: Add Group

Policy Settings

Enable Policy

Policy Name: ? (e.g. my IT policy)

Description:

(Maximum allowed characters 256)

Insert Above Policy:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Identification Profile:

Authorized Users and Groups [Add Identification Profile](#)

All Authenticated Users

Selected Groups and Users ?
Groups: No groups entered
Users: No users entered

[Cancel](#) [Submit](#)

図 - ルーティングポリシーへのIDプロファイルの追加

ステップ 5.3 : アップストリームプロキシを使用する希望の条件については、Routing Destinationリンクをクリックし、ステップ3で作成したアップストリームプロキシグループを選択します。

Routing Policies

Order	Members	Routing Destination	IP Spoofing	Clone Policy	Delete
1	Partial Routing Policy Identification Profile: Upstream Proxy ID Profile All identified users	(global policy)	(global policy)		
	Global Routing Policy	Direct Connection	Do not use IP Spoofing		

5.3

図 : ルーティング宛先の設定



注 : アップストリームプロキシを使用するすべてのトラフィックが必要な場合は、グローバルルーティングポリシーから目的のアップストリームプロキシを選択します。

ステップ 5.4 : 変更を [Submit] して [Commit] します。

ステップ6: (オプション) アップストリームプロキシ応答しないタイムアウト設定の設定



ヒント:これらの値の動作と潜在的な影響を十分に理解していない限り、これらの値を変更しないことを推奨します。

ステップ 6.1 : CLIにログインし、advancedproxyconfigを実行します。

ステップ 6.2 : MISCELLANEOUSを選択します。

ステップ 6.3 : 「Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds). 」が表示されるまでEnterキーを押します。最小時間を設定できます。SWAは以前にSickと宣言されたアップストリームプロキシの再試行を待機します。デフォルト値は 10 秒です。

ステップ 6.4 : Enterキーを押して、次の設定に進みます。応答しないアップストリームプロキシをチェックするための最大アイドルタイムアウトを定義する際に、このタイムアウト値に達してから再接続の試行が設定済みの回数を使い果たす(ステップ3)と、SWAはアップストリームプロキシをオフラインであると思なすことに注意してください。

ステップ 6.7 : Enterキーを押し続け、ウィザードを終了するまでcommitを実行して変更を保存します。


アクセスログ

アクセスログでは、アップストリームプロキシにルーティングされたトラフィックは、DEFAULT_PARENTとして表示され、その後にアップストリームプロキシの名前が続きます。次に例を示します。

```
1775659642.780 462 10.20.3.15 TCP_MISS_SSL/200 129 CONNECT tunnel://www.cisco.com:443/ "AMojARRA\amojar
```


Proxylogs


プロキシログから、アップストリームプロキシのヘルスステータスを確認できます。

 ヒント:peerをフィルタリングして、アップストリームプロキシに関連するログを確認できます。

次に例をいくつか示します。これは、ステップ3で再接続の試行を2回設定しており、2回アップストリームプロキシへの接続が失敗した後で、アップストリームプロキシがdadと宣言され、プロキシプロセスが再起動されるまで、SWAはこのアップストリームプロキシをリストから削除します。

```
Thu Apr  2 13:52:35 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer-upstream 10.48.48.182:3128 was hea
Thu Apr  2 13:52:36 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer 10.48.48.182:3128 was sick, now he
...
Thu Apr  2 13:59:37 2026 Info: PROX_CONNTRACK : 60 : [71197:0] Peer 10.48.48.183:3128 remains sick afte
Thu Apr  2 13:59:39 2026 Warning: PROX_CONNTRACK : 70 : [71197:0] Peer-upstream 10.48.48.183:3128 decla
```

 注: アップストリームプロキシがTCP SYN要求に応答しない、HTTP応答コードの返に失敗する、またはHTTP 504 (ゲートウェイタイムアウト) 応答を返す場合、SWAはアップストリームプロキシが使用不可能と見なし、そのステータスを正常から異常に変更します。

 ヒント:SWAは、VIAヘッダーを返す場合、アップストリームプロキシが正常であると見なし、そのステータスを正常から異常に変更しません。

関連情報

- [AsyncOS 15.0 for Cisco Secure Web Appliance ユーザガイド](#)

- [Secure Web ApplianceでのカスタムURLカテゴリの設定：シスコ](#)
- [Cisco Webセキュリティアプライアンス\(WSA\)でOffice 365トラフィックを認証および復号化から除外する方法：シスコ](#)
- [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：シスコ](#)
- [Secure Web Applianceでのトラフィックのブロック](#)
- [セキュアWebアプライアンスでのアップロードトラフィックのブロック](#)
- [SWAでの実行可能ファイルのダウンロードのブロック](#)
- [Secure Web ApplianceでのMicrosoft Updatesトラフィックのバイパス](#)
- [Secure Web Applianceでの認証のバイパス：シスコ](#)

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。