

# Secure Web Applianceでのトラフィックのバイパス

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[さまざまなタイプのバイパス](#)

[導入タイプ別のSWAバイパス手順](#)

[明示的な展開でのトラフィックのバイパス](#)

[PACファイルの設定](#)

[ブラウザの設定\(Microsoft Edge、Internet Explorer、Google Chrome\)](#)

[ブラウザ設定\(Mozilla FireFox\)](#)

[ブラウザの設定\(Apple Safari\)](#)

[グループポリシーの設定](#)

[TransparentDeploymentでのトラフィックのバイパス](#)

[SWAバイパス設定](#)

[WCCP/PBRルータからのトラフィックのリダイレクト](#)

[SWAでのパススルーの設定とトラフィックの許可](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Secure Web Appliance(SWA)でトラフィックをバイパス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

## 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。

## さまざまなタイプのバイパス

SWAでは、トラフィックがSWAに到達するのをバイパスする3つの異なる概念があります。これらは、プロキシの導入(明示的または透過的な導入)によって異なります。また、SWAによる分析とスキャンの対象にもなります。次に、これら3つの概念の概要を示します。

- **バイパス** : トラフィックがSWAに到達するのを防止する設定。これにより、ネットワークインターフェイスカード(NIC)の使用率が低下し、ユーザとアプライアンス間のセッションが不要になります。
- **パススルー** : この設定は、SWAによるHTTPSトラフィックの復号化を防止します。それでも、SWAでは、クライアントとSWAの間のセッションと、SWAとWebサーバの間のセッションの2つのセッションが引き続き促進されます。
- **Allow** : アクセスポリシー内で、HTTPまたは復号化されたトラフィックが、AMP、Sophos、WebRoot、アプリケーションフィルタなどの内部SWAエンジンによる検査をスキップする設定。この場合でも、SWAでは2つのセッションが使用されています。

Type	Applies to	Transparent Deployment	Explicit Deployment	Configuration Path	Logging	Number of Sessions	Description
Bypass from SWA	HTTPS & HTTP	✓	✗	GUI > Web Security Manager > Bypass Settings	Bypasslogs	1	SWA routes the traffic to configured gateway (Layer 3 redirection)
Bypass from WCCP Router	HTTPS & HTTP	✓	✗	WCCP Router	No Logs on SWA	0	Traffic Redirects to the Gateway from Router
Bypass from PAC	HTTPS & HTTP	✗	✓	From the PAC file	No Logs on SWA	0	Requests are not sent to the proxy.
Bypass from Browser	HTTPS & HTTP	✗	✓	From the Browser or Group Policy	No Logs on SWA	0	Requests are not sent to the proxy.
Pass Through	HTTPS & HTTP	✓	✓	GUI > Web Security Manager > Decryption Policy	Accesslogs	2	SWA does not decrypt the traffic and sends the same ClientHello to the web server.
Allow	Decrypted Traffic & HTTP	✓	✓	GUI > Web Security Manager > Access Policy	Accesslogs	2	SWA does not Scan the traffic with its scanning engines, such as AMP, Sophos, WebRoot, AVC and ...

図 - 比較表

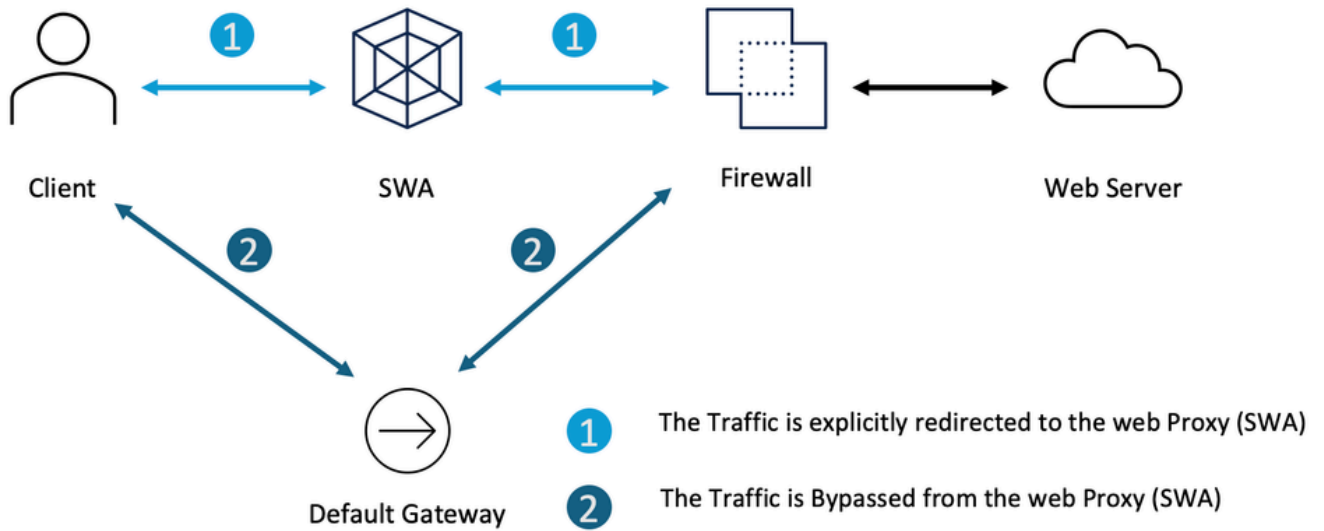
## 導入タイプ別のSWAバイパス手順

バイパスの手順は、プロキシ導入モデルによって異なります。各タイプの概要を次に示します。

- 明示的な導入：クライアントは、トラフィックをプロキシに転送するように手動で設定されます。
- 透過的な導入：ネットワークインフラストラクチャはトラフィックをプロキシに自動的にリダイレクトするため、クライアント側の設定は必要ありません。

### 明示的な展開でのトラフィックのバイパス


Explicit Deploymentでトラフィックをバイパスするには、目的のURLのWeb要求をSWAに転送しないようにクライアントを設定する必要があります。このネットワーク図に示すように、一部のトラフィックはファイアウォールまたはデフォルトゲートウェイに直接送信され、SWA (パス番号2) をバイパスします。

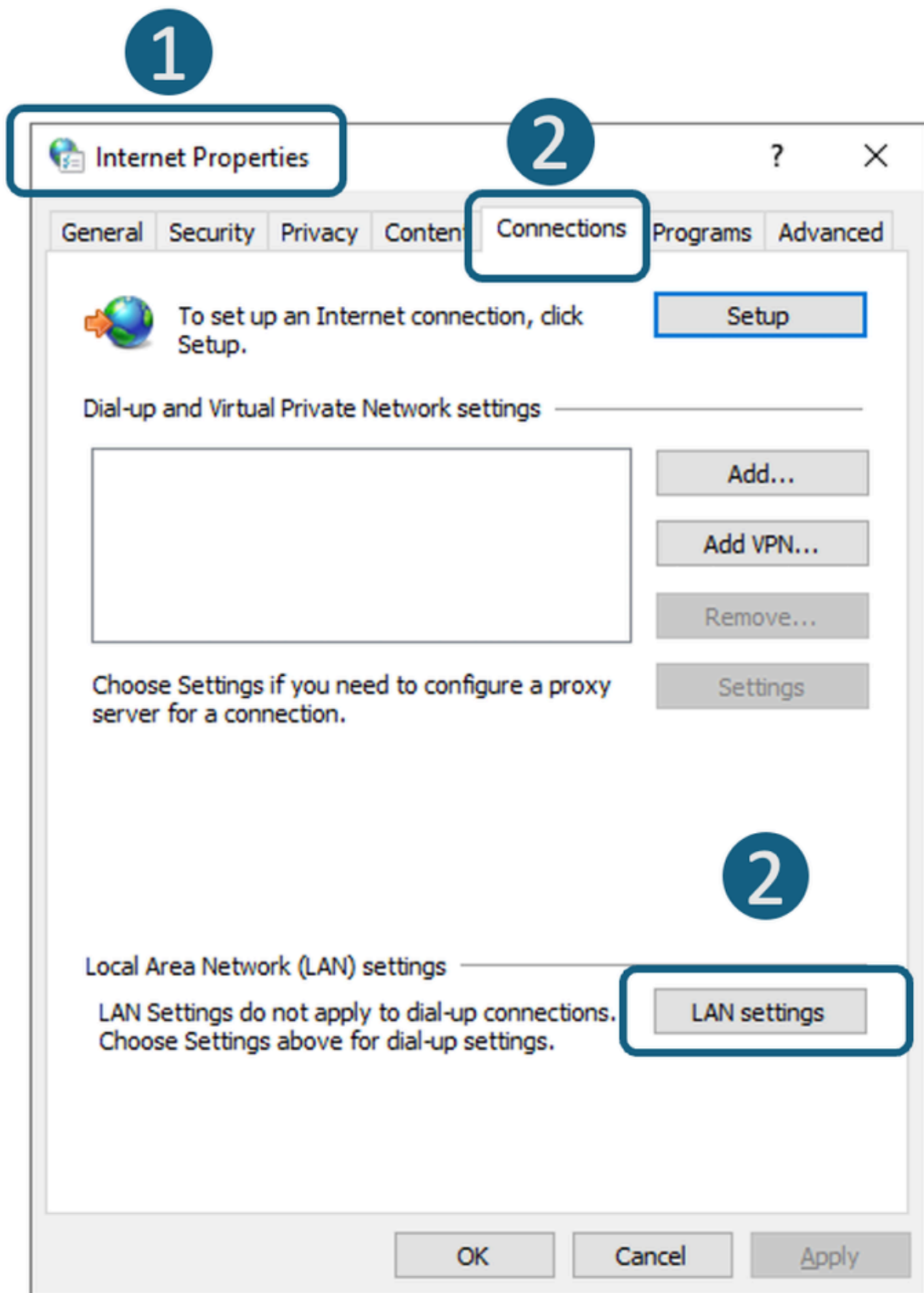


イメージ：明示的な導入でのトラフィックのバイパス

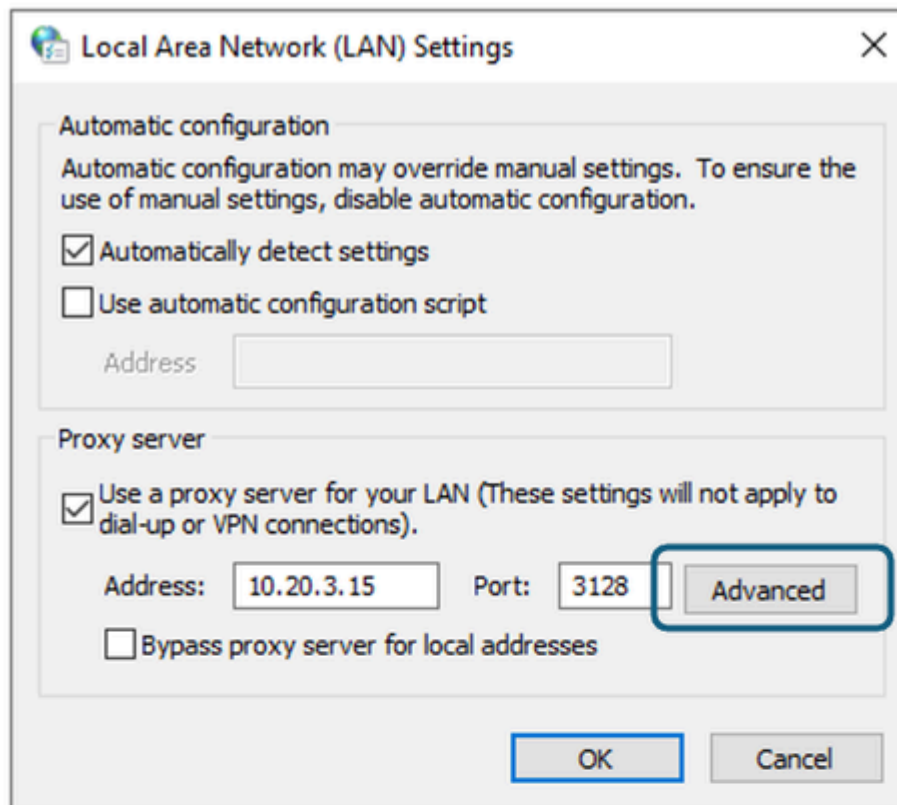
明示的なプロキシ導入に応じて、一部のURLをSWAにリダイレクトされないように除外できます。

<p>明示的なプロキシ設定</p>	<p>SWAに到達するURLを除外する手順</p>
<p>PACファイルの設定</p>	<p>PACファイルの設定方法に応じて、例外リストを定義し、アクションをDIRECTに設定できます。</p> <p>プライベートIPアドレスがSWAに到達するのをバイパスするサンプルを示します</p> <pre>var resolved_ip = dnsResolve(host); if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0")        isInNet(resolved_ip, "172.16.0.0", "255.240.0.0")        isInNet(resolved_ip, "192.168.0.0", "255.255.0.0")        isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return "DIRECT";</pre> <p>これは、SWAのリダイレクトから<a href="http://www.cisco.com">www.cisco.com</a>へのトラフィックをバイパスする例です</p> <pre>if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";</pre> <p>この例では、cisco.comのすべてのサブドメインをバイパスして、SWAをリダイレ</p>

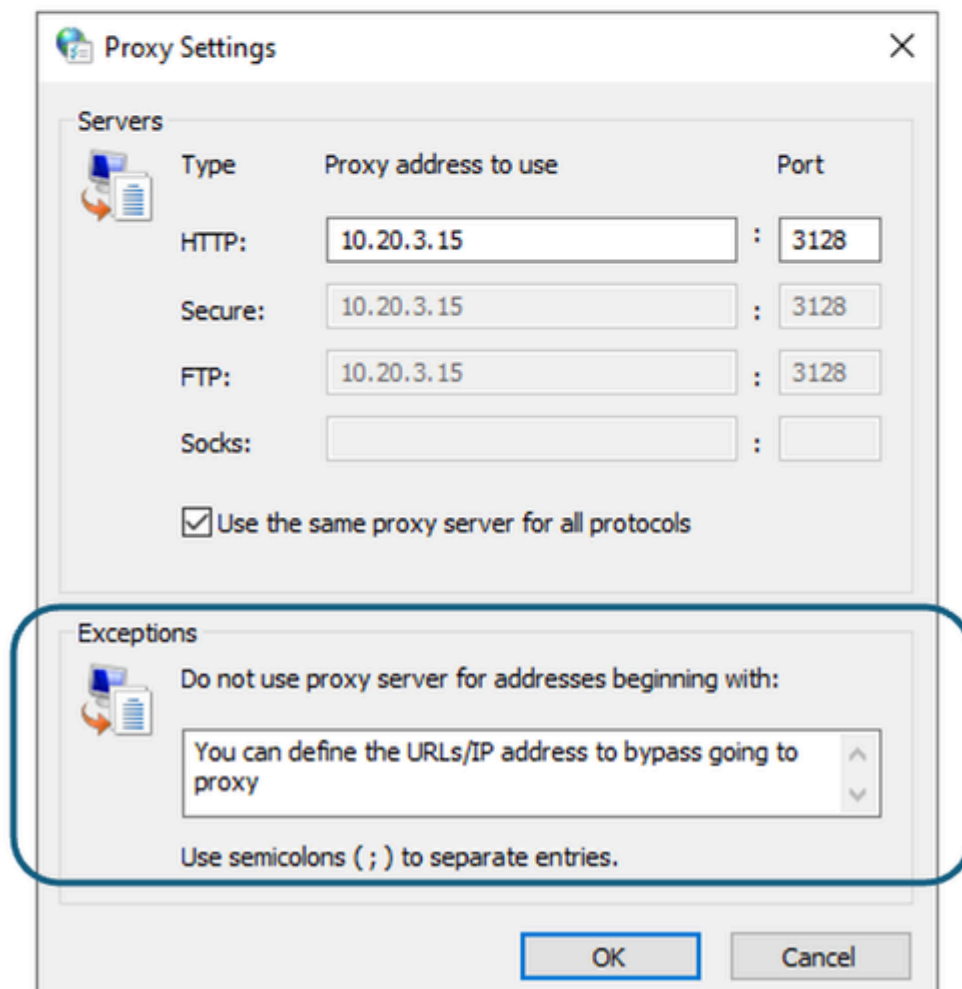
	<p>クトします</p> <pre>if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";</pre> <p> 注:PACファイルはシスコ製品のファイルではないため、便宜上、この情報を提供しています。さらにサポートが必要な場合は、ソフトウェアのベンダーに連絡してください。</p>
<p>ブラウザの設定(Microsoft Edge、Internet Explorer、Google Chrome)</p>	<p>ステップ 1 : スタートメニューで「インターネットオプション」と入力して Enterキーを押します</p> <p>ステップ 2Connectionsタブに移動し、LAN Settingsをクリックします</p> <p>ステップ 3Advanced</p> <p>ステップ 4 「例外」セクションで必要なURLを定義します。</p>



イメージ - Lan設定に移動します



3



4

ブラウザ設定  
(Mozilla  
FireFox)

ステップ 1 : 右上隅の3つのバーメニューをクリックし、Settingsを選択します。  
ステップ 2 検索バーに「proxy」と入力します。  
ステップ 3 No Proxy forセクションで必要なURLを定義します。

Connection Settings

Configure Proxy Access to the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration

HTTP Proxy  Port

Also use this proxy for HTTPS

HTTPS Proxy  Port

SOCKS Host  Port

SOCKS v4  SOCKS v5

Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24  
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

Do not prompt for authentication if password is saved

Proxy DNS when using SOCKS v4

Proxy DNS when using SOCKS v5

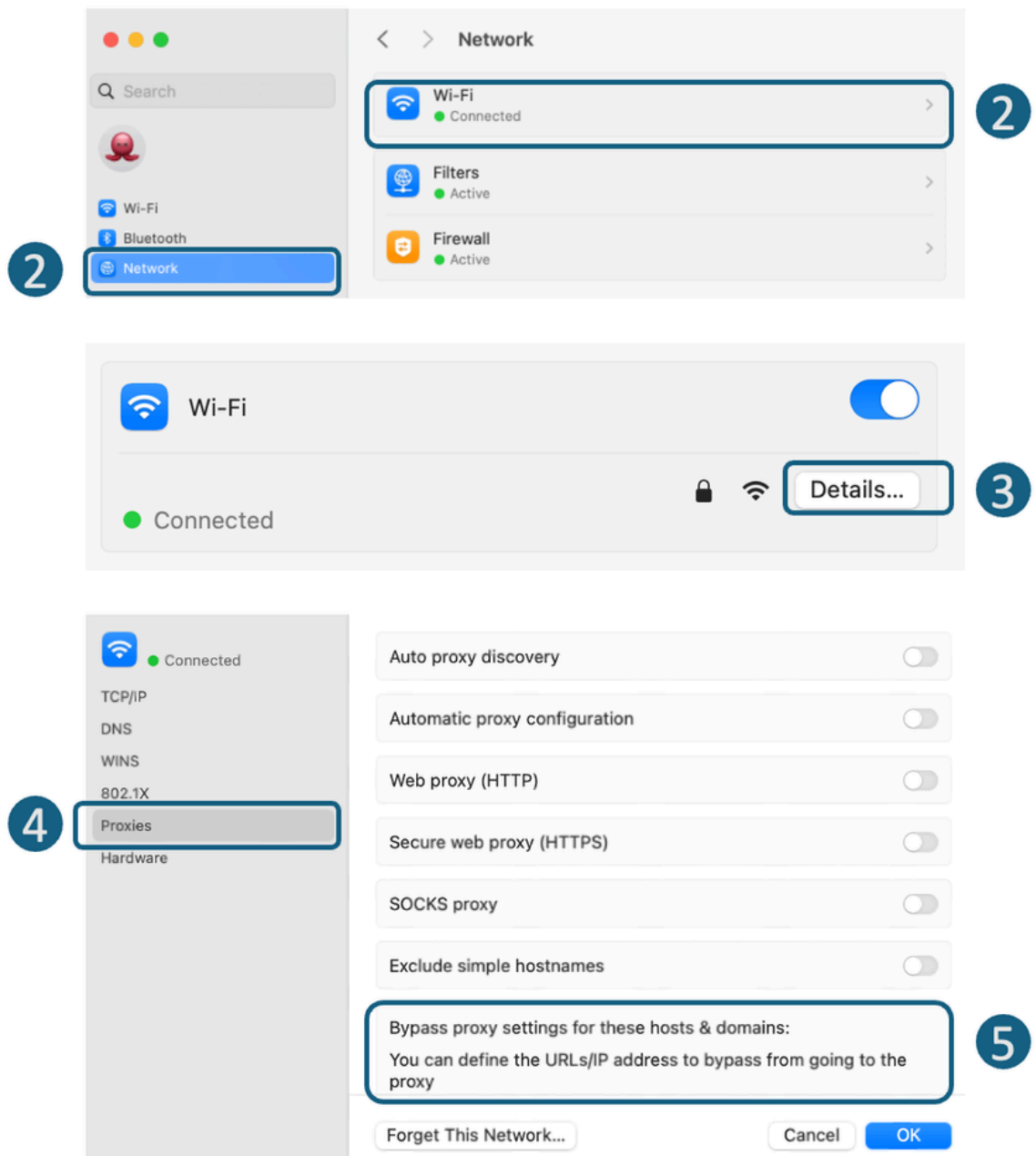
イメージ : Fire Foxでの例外の定義

ブラウザの設  
定(Apple  
Safari)

ステップ 1 : 左上隅のAppleアイコンをクリックして、System Settingsを選択しま  
す。  
ステップ 2 左側のパネルでNetworkに移動し、インターネットへのアクセスに使用  
しているネットワークインターフェイスを選択します。  
ステップ 3 Detailsをクリックします。

ステップ 4 左側のパネルからProxiesを選択します。

ステップ 5 Bypass Proxy Settingsセクションで、必要なURLを定義します。



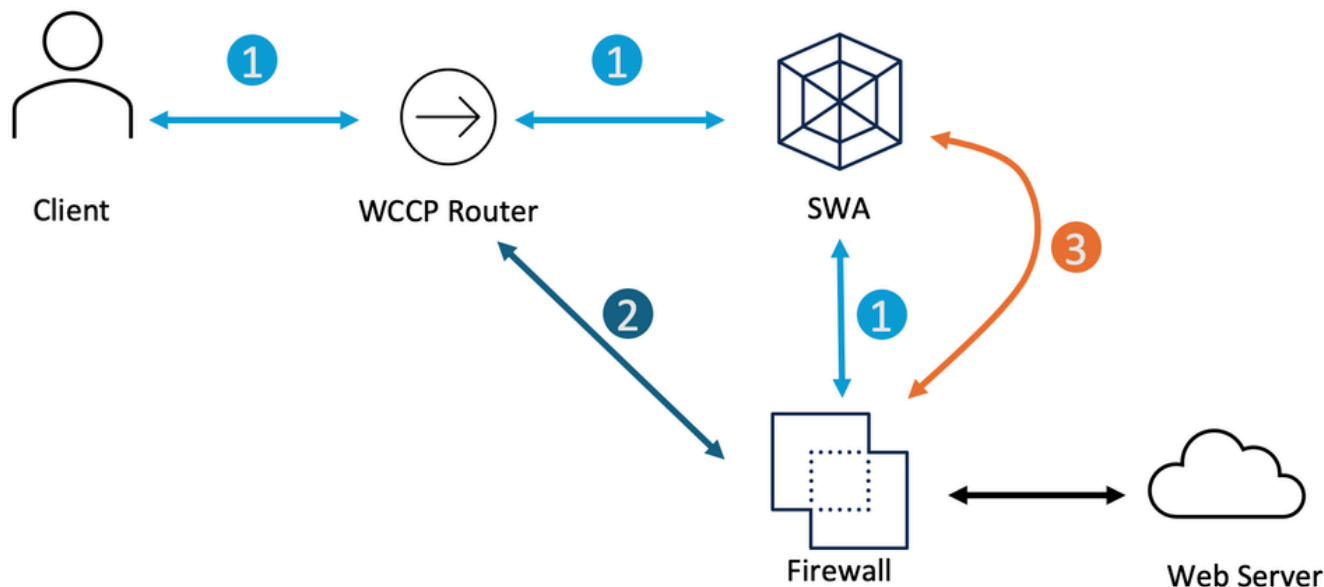
イメージ : Fire Foxでの例外の定義

グループポリシーの設定

プロキシ設定をプッシュするためのグループポリシーの設定方法に応じて、例外リストを定義できます。

透過的な導入でのトラフィックのバイパス

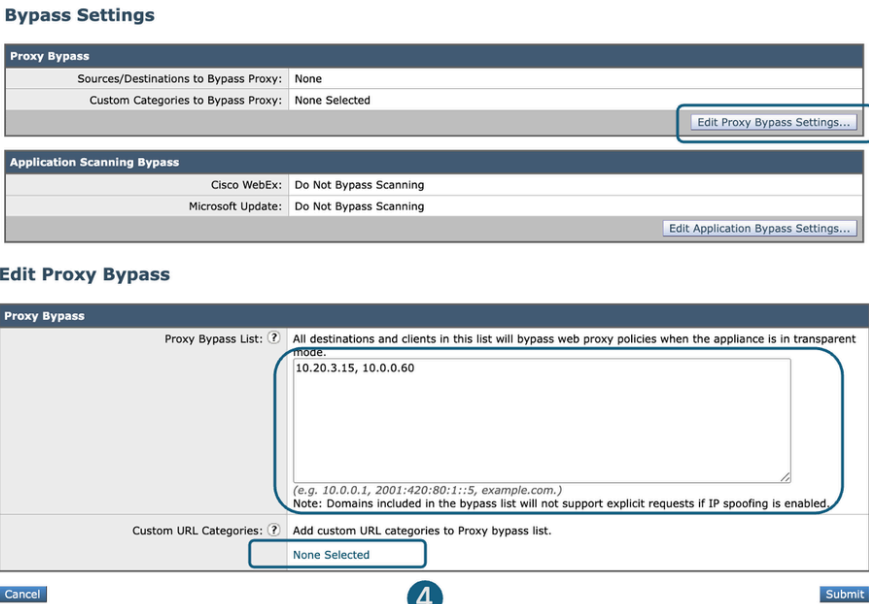

透過型導入では、WCCPルータまたはSWAバイパス設定を使用してトラフィックをバイパスできます。SWAバイパスはレイヤ3で機能し、トラフィックをデフォルトゲートウェイにルーティングしてアプライアンス全体をバイパスするため、処理と個別のセッションの作成ができなくなります。



- 1 The Traffic is Transparently redirected to the SWA
- 2 The Traffic is Redirected from the WCCP Router, to not go to the SWA
- 3 The Traffic is Bypassed in the SWA as a layer 3 traffic and routes to the SWA Default Gateway

イメージ：透過型導入でのトラフィックのバイパス

<p>トラフィックのバイパス透過型プロキシの導入</p>	<p>トラフィックがSWAに到達するのをバイパスする手順</p>
<p>SWAバイパス設定</p>	<p>ステップ 1 : GUIから、Web Security Managerを選択します。</p> <p>ステップ 2 Bypass Settingsを選択します。</p> <p>ステップ 3 Edit Proxy Bypass Settingsをクリックします。</p> <p>ステップ 4 URL、IPアドレスを入力するか、カスタムURLカテゴリをリストに追加できます。</p> <p>ステップ 5変更を [Submit] して [Commit] します。</p>

	 <p>☒ - バイパス設定の設定</p> <p> ヒント：この設定でバイパスされるトラフィックはアクセスログには記録されず、Bypass_Logsで確認できます。</p>
<p>WCCP/PBRルータからのトラフィックのリダイレクト</p>	<p>一部のトラフィックをSWAにリダイレクトしないように、WCCPまたはPolicy Based Router ( PBR ; ポリシーベースルータ ) で送信元または宛先のIPアドレスを設定できます。</p>

## SWAでのパススルーの設定とトラフィックの許可

トラフィックがSWAに到達している場合、プライバシー上の問題が原因でSWAの負荷を軽減するために、一部のURLのトラフィックをSWAで検査しないようにするには、次の手順を使用します。

手順	手順
<p>ステップ 1 : URLのカスタムURLカテゴリを作成します。</p>	<p>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。          手順1.3:一意のCategoryNameを割り当てます。</p>

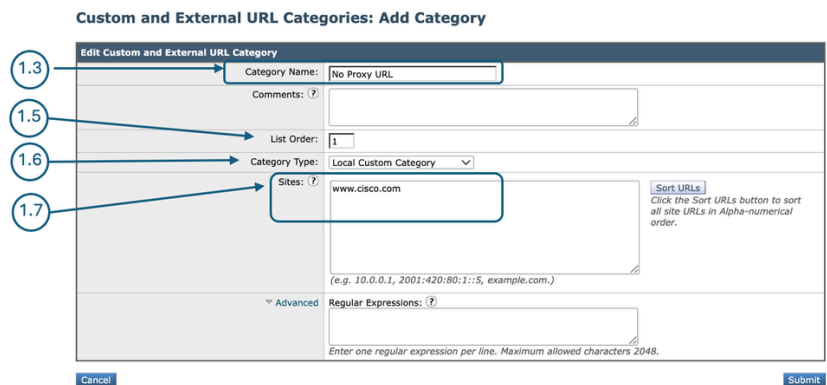
ステップ1.4: ( オプション ) 説明を追加する。

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セクションに目的のURLを追加します。

ステップ 1.8 : [Submit] をクリックします。



イメージ - カスタムURLカテゴリの作成

ステップ 2 認証からトラフィックを除外するIDプロファイルを作成します。

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 : ユーザ識別方法セクションで、認証/識別から免除を選択します。

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 : Advancedセクションから、Custom URL Categoriesを選択します。

### Identification Profiles: Add Profile

2.4

2.6

2.7

2.9

イメージ - 識別プロファイルの追加

ステップ 2.10 : ステップ1で作成したカスタムURLカテゴリを追加します。

ステップ 2.11 : [Done] をクリックします。

ステップ 2.12 : [Submit] をクリックします。

ステップ 3 トラフィックを通過させる復号化ポリシーを作成します。

ステップ 3.1: GUI から、Web Security Manager を選択し、Decryption Policy をクリックします。

ステップ 3.2 : Add Policies をクリックして、復号ポリシーを追加します。

ステップ 3.3 : このポリシーを有効にするには、Enable Policy チェックボックスを使用します。

手順 3.4: 一意の PolicyName を割り当てます。

ステップ 3.5: (任意) 説明を追加する。

ステップ 3.6: Insert Above Policy policy ドロップダウンリストから、最初のポリシーを選択します。

ステップ 3.7: ID プロファイルおよびユーザから、ステップ 2 で作成した ID プロファイルを選択します。

ステップ 3.8 : [Submit] をクリックします。

### Decryption Policy: Add Group

イメージ：復号化ポリシーの作成

ステップ3.9:復号ポリシーページのURLフィルタリングで、この新しい復号ポリシーに関連付けられているリンクをクリックします。

### Decryption Policies

Success — The policy group "DP Pass Through" was added.

Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DP Pass Through Identification Profile: No Auth ID All identified users	Monitor: 1	(global policy)	(global policy)		
	<b>Global Policy</b> Identification Profile: All	Pass Through: 0 Monitor: 0 Decrypt: 0 Drop: 0 Time-Based: 0 Quota-Based: 0	Not Available	Decrypt		

Callout 3.9 points to the 'Monitor: 1' link in the URL Filtering column of the first row.

図 - URLフィルタリングの選択

ステップ3.10:SelectPassスルーには、ステップ1で作成したURLカテゴリのアクションがあります。

### Decryption Policies: URL Filtering: DP Pass Through

Custom and External URL Category Filtering

Add, edit, reorder or delete categories in the Custom and External URL Categories list.

Category	Category Type	Use Global Settings	Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
No Proxy URL	Custom (Local)	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	(Unavailable)	(Unavailable)

Callout 3.10 points to the 'Pass Through' checkbox in the 'No Proxy URL' row.

イメージ：パススルーするアクションの設定

ステップ 3.11 : [Submit] をクリックします。

ステップ 4Microsoft Updatesトラフィックを許可するアクセスポリシーを作成します。

ステップ4.1:GUIから、Web Security Managerを選択し、Access Policyをクリックします。

ステップ 4.2 : アクセスポリシーを追加するには、Add Policiesをクリックします。

ステップ4.3 : このポリシーを有効にするには、Enable Policyチェックボックスを使用します。

手順4.4:一意のPolicyNameを割り当てます。

ステップ4.5: ( 任意 ) 説明を追加する。

ステップ4.6:Insert Above Policypolicyドロップダウンリストから、最初のポリシーを選択します。

ステップ4.7:Identification Profiles and Usersから、ステップ2で作成したIdentification Profileを選択します。

ステップ 4.8 : [Submit] をクリックします。

**Access Policy: Add Group**

**Policy Settings**

Enable Policy

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

Description:   
(Maximum allowed characters 256)

Insert Above Policy: 1 (Global Policy)

Policy Expires:   
 Set Expiration for Policy  
On Date: MM/DD/YYYY  
At Time: 00 : 00

**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: Select One or More Identification Profiles

Identification Profile	Authorized Users and Groups	Add Identification Profile
No Auth ID	No authentication required	<input type="button" value="Add Identification Profile"/>

Advanced Define additional group membership criteria.

Cancel Submit

イメージ : アクセスポリシーの作成

ステップ 4.9 : Access PoliciesページのURL Filteringの下で、この新しいアクセスポリシーに関連付けられているリンクをクリックします。

**Access Policies**

Success — The policy group "AP Allow" was added.

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	AP Allow Identification Profile: No Auth ID All identified users.	(global policy)	Monitor: 1	(global policy)	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Block: 0 Warn: 0 Monitor: 0 Allow: 0 Redirect: 0 Time-Based: 0 Quota-Based: 0	Not Available	No blocked items	Secure Endpoint: Enabled	None		

Edit Policy Order...

図 - URLフィルタリングの選択

ステップ4.10:Select Allowasは、ステップ1で作成したURLカテゴリ用に作成したカスタムURLカテゴリのアクションです。

Custom and External URL Category Filtering		Use Global Settings		Override Global Settings					
Category	Category Type	Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based	
No Proxy URL	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)	

4.10

イメージ：許可するアクションの設定

ステップ 4.11：[Submit] をクリックします。

ステップ 4.12：変更を確定します。

## 関連情報

- [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](#)
- [AsyncOS 15.0 for Cisco Secure Web Applianceユーザガイド – GD \(一般導入\) – ポリシーアプリケーションのエンドユーザの分類\[Cisco Secure Web Appliance\] – シスコ](#)
- [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](#)

## 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。