Secure Web Applianceでのトラフィックのバイパス

内容

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キ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

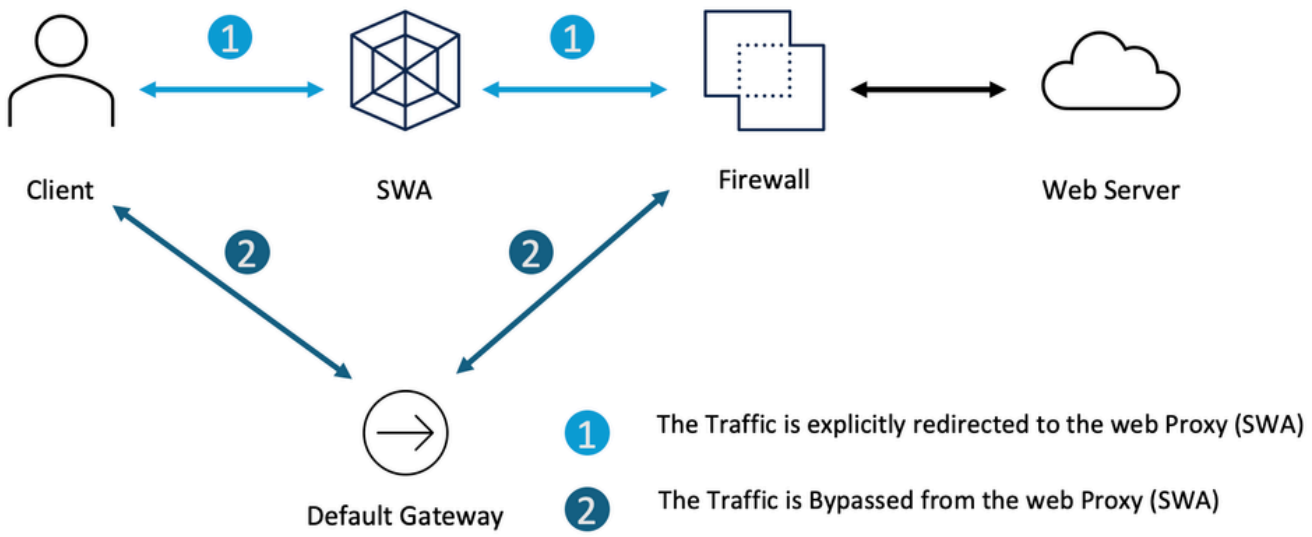
導入タイプ別のSWAバイパス手順

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。



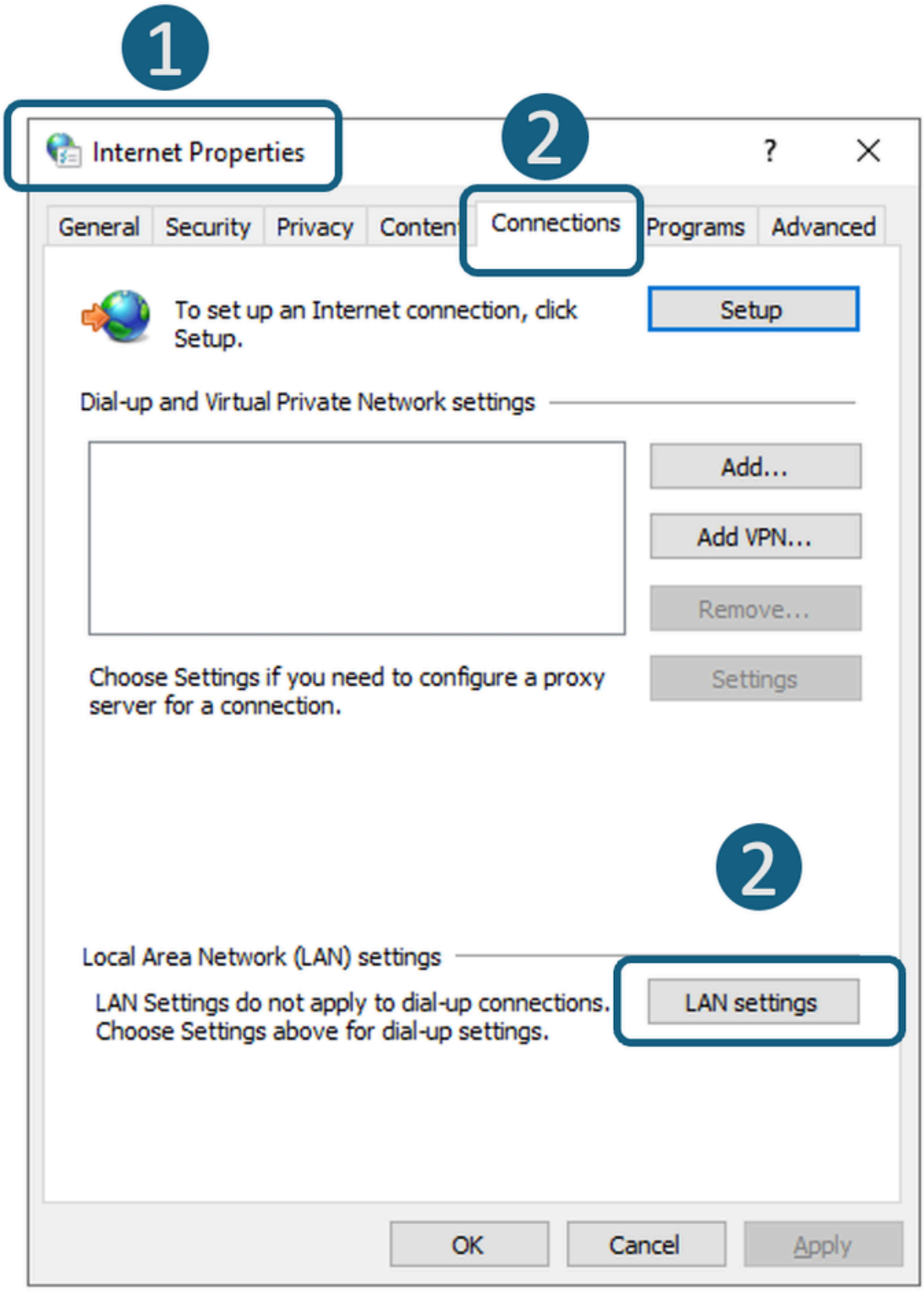
イメージ：明示的な導入でのトラフィックのバイパス

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。

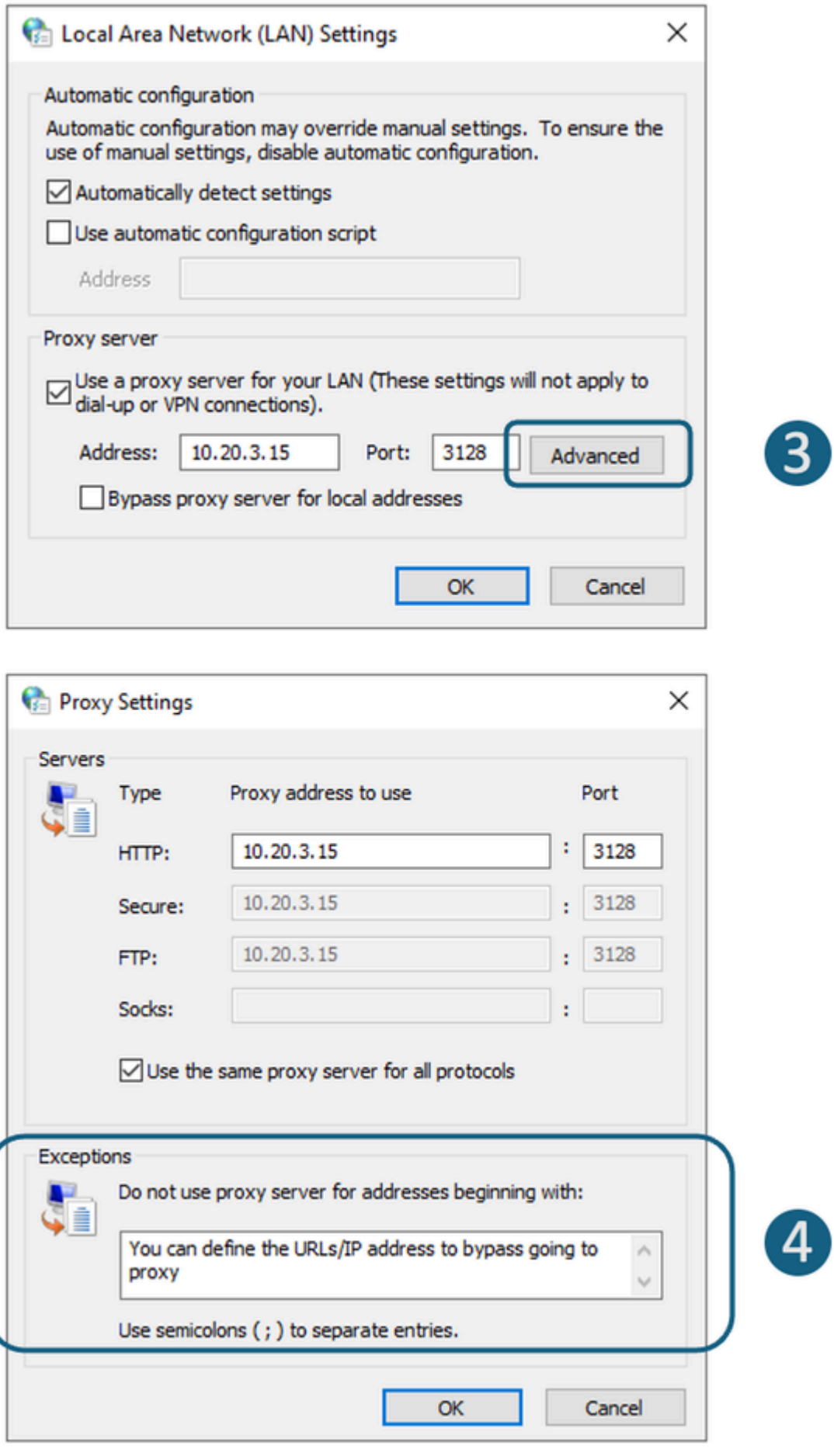
明示的なプロキシ設定	SWAに到達するURLを除外する手順

PACファイルの設定	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。
	
	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次に示します
	
	`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";`
	
	これは、SWAのリダイレクトからwww.cisco.comへのトラフィックをバイパスする例です
	
	`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`
	
	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

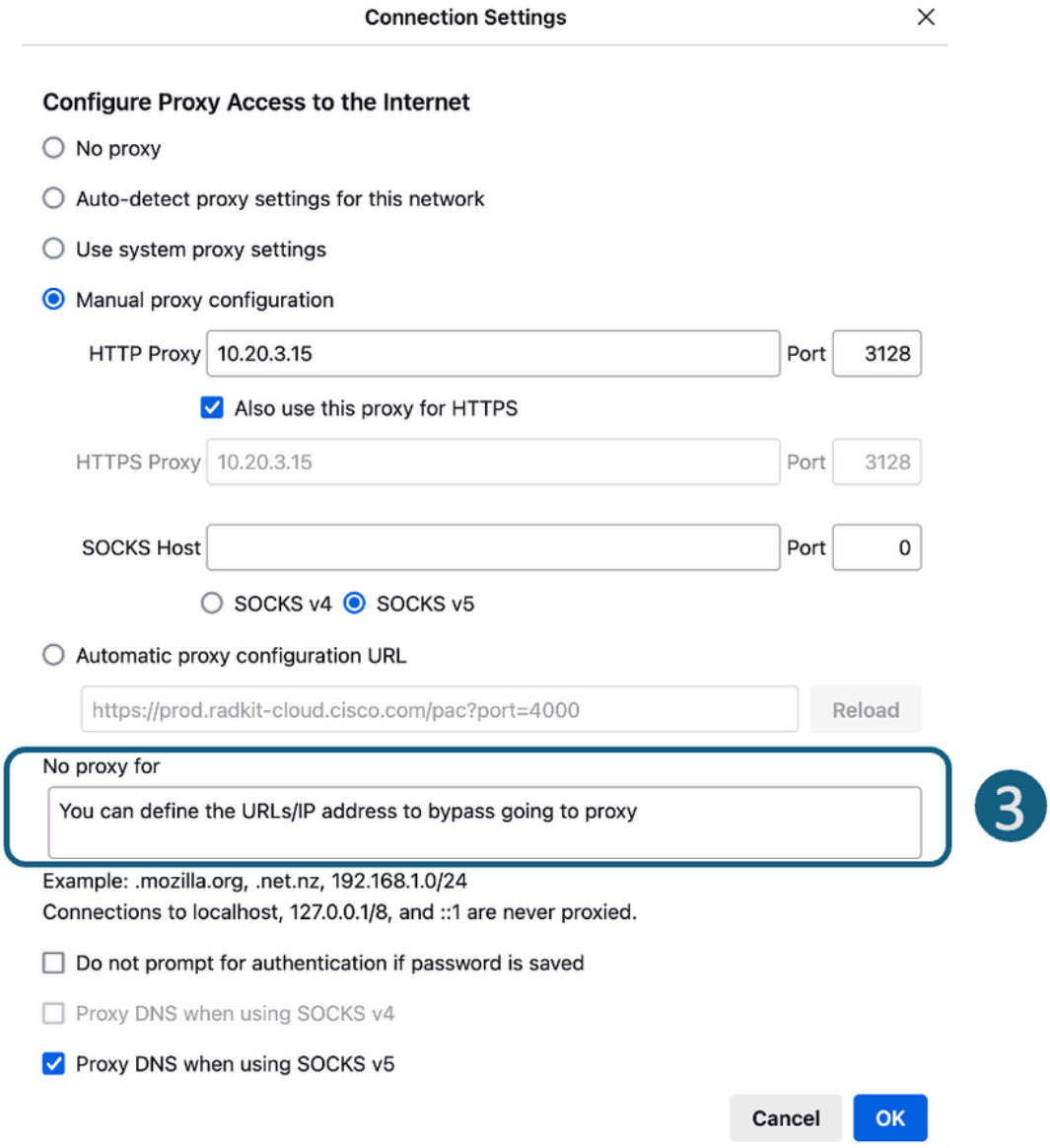
	クトします `if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";` 注:PACファイルはシスコ製品のファイルではないため、便宜上、この情報を提供しています。さらにサポートが必要な場合は、ソフトウェアのベンダーに連絡してください。
ブラウザの設定(Microsoft Edge、Internet Explorer、Google Chrome)	ステップ 1：スタートメニューで「インターネットオプション」と入力してEnterキーを押します ステップ 2Connectionsタブに移動し、LAN Settingsをクリックします ステップ 3Advanced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

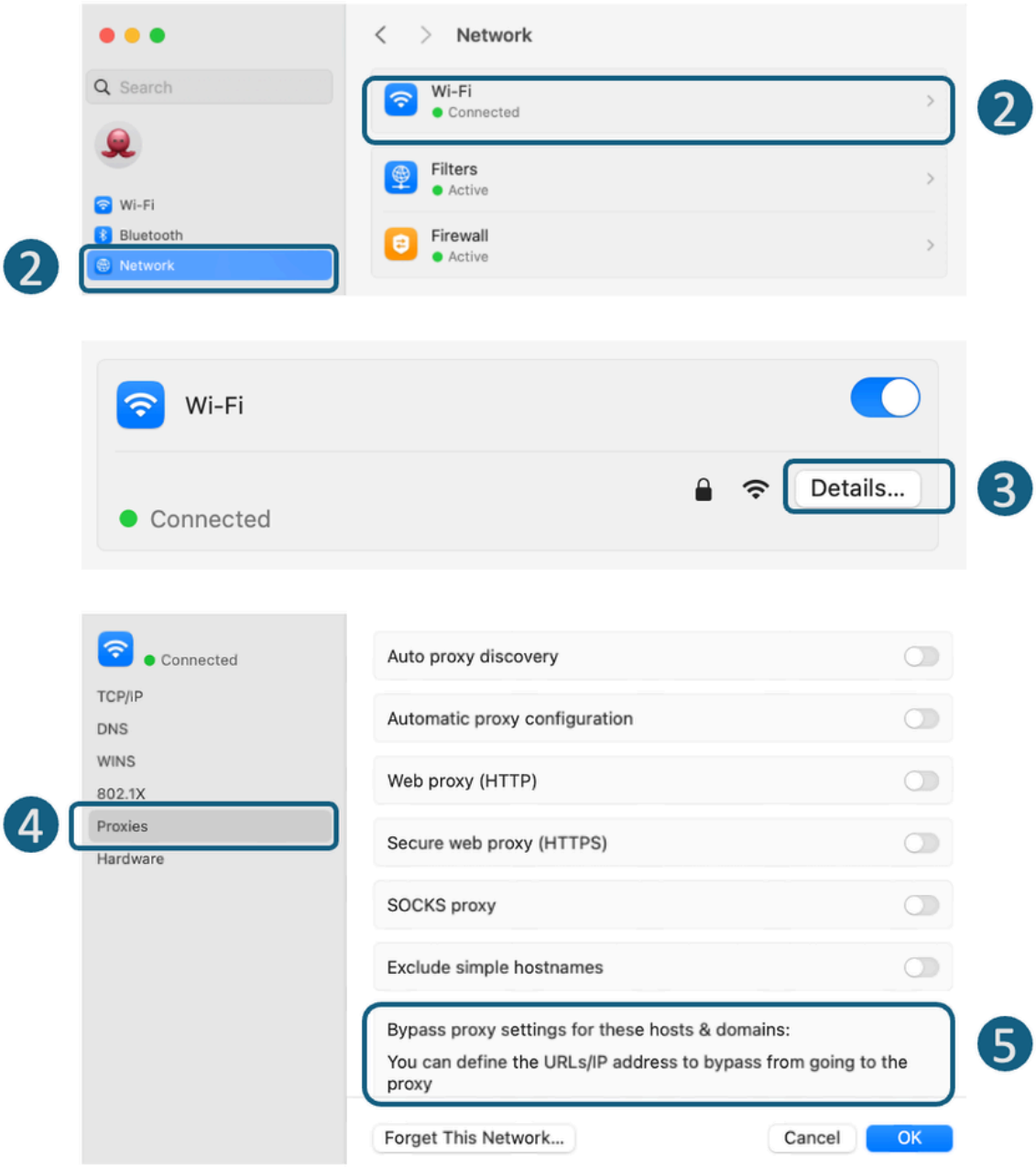


イメージ – Lan設定に移動します


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: 10.20.3.15
Port: 3128
Advanced
Bypass proxy server for local addresses
OK
Cancel
3
Proxy Settings
Servers
Type
Proxy address to use
Port
HTTP: 10.20.3.15 : 3128
Secure: 10.20.3.15 : 3128
FTP: 10.20.3.15 : 3128
Socks: :
Use the same proxy server for all protocols
Exceptions
Do not use proxy server for addresses beginning with:
You can define the URLs/IP address to bypass going to proxy
Use semicolons (;) to separate entries.
OK
Cancel
4

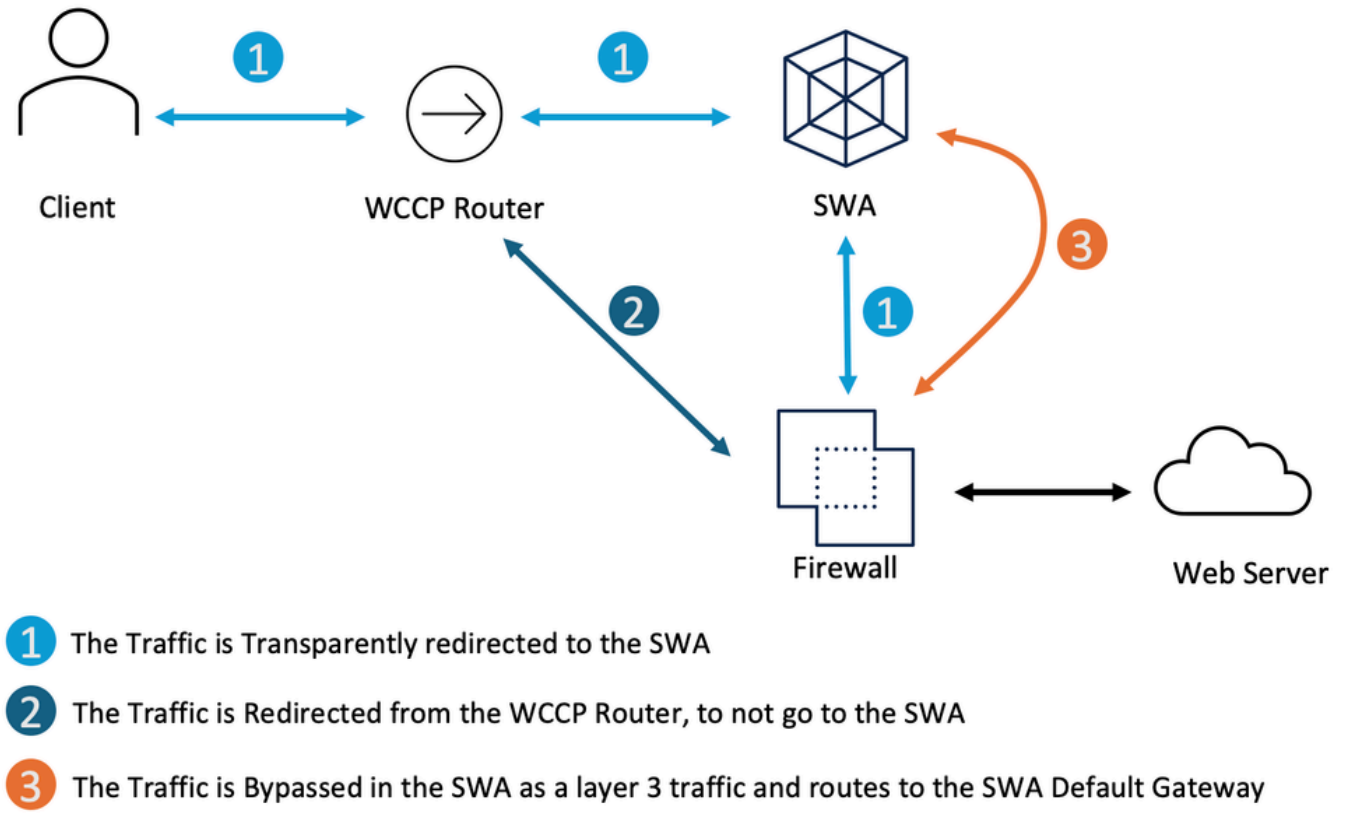
イメージ：例外の定義

ブラウザ設定(Mozila 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。  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 3Details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。

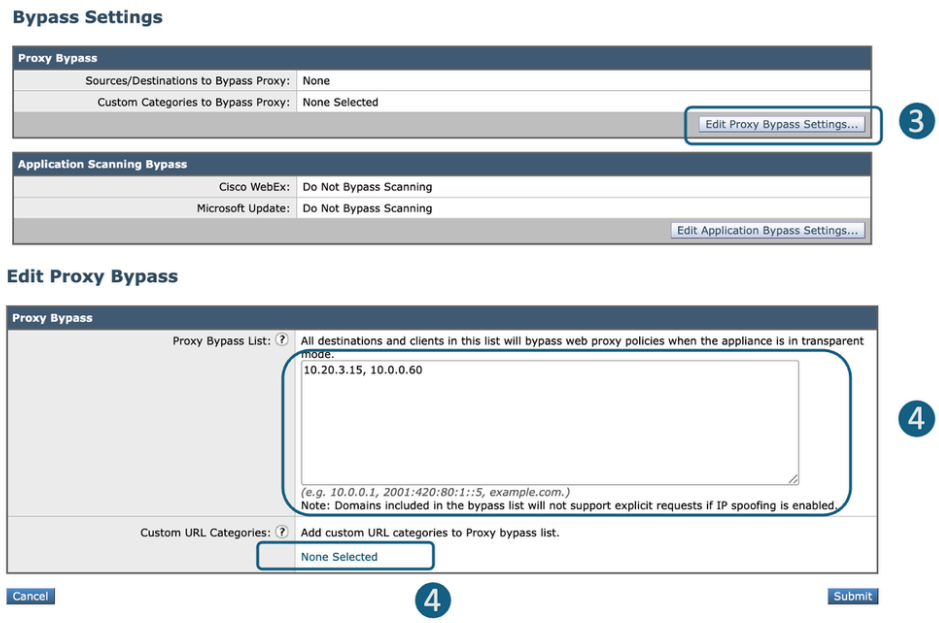
透過的な導入でのトラフィックのバイパス

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。



イメージ：透過型導入でのトラフィックのバイパス

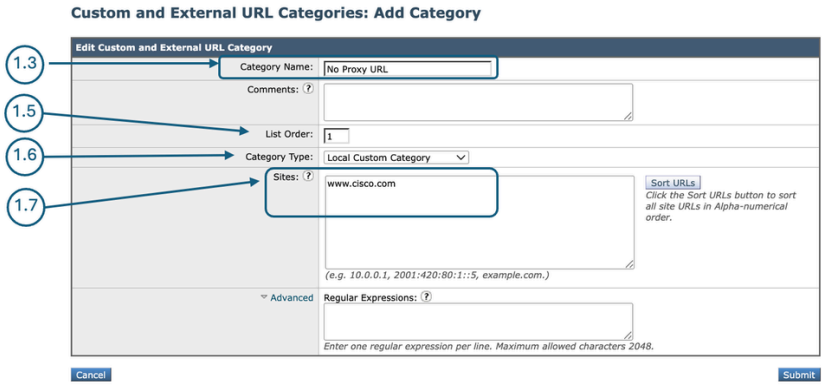
トラフィックのバイパス透過型プロキシの導入	トラフィックがSWAに到達するのをバイパスする手順
SWAバイパス設定	ステップ 1：GUIから、Web Security Managerを選択します。 ステップ 2Bypass Settingsを選択します。 ステップ 3 Edit Proxy Bypass Settingsをクリックします。 ステップ 4 URL、IPアドレスを入力するか、カスタムURLカテゴリをリストに追加できます。 ステップ 5変更を [Submit] して [Commit] します。

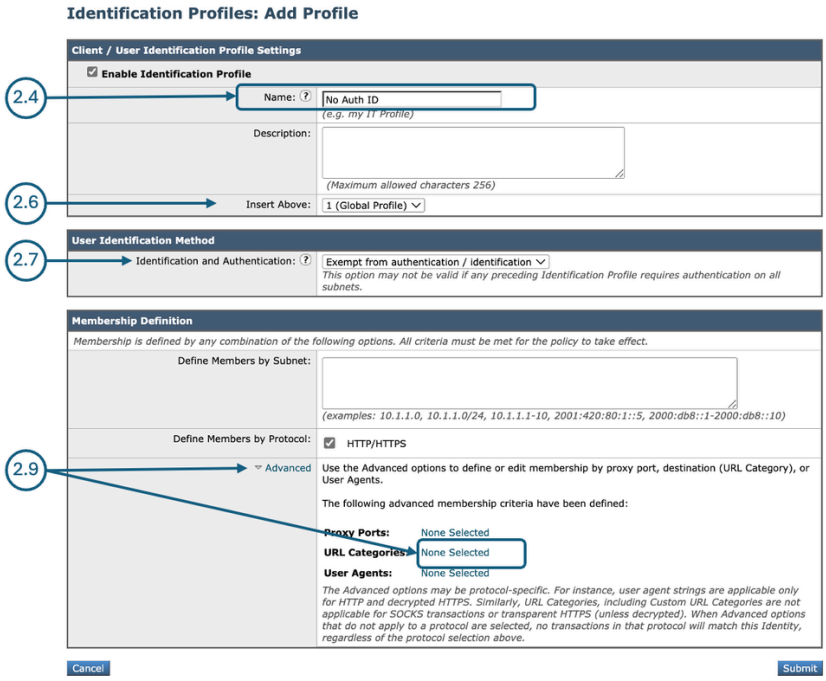
	 図 – バイパス設定の設定 ヒント：この設定でバイパスされるトラフィックはアクセスログには記録されず、Bypass_Logsで確認できます。
WCCP/PBRルータからのトラフィックのリダイレクト	一部のトラフィックをSWAにリダイレクトしないように、WCCPまたはPolicy Based Router（PBR；ポリシーベースルータ）で送信元または宛先のIPアドレスを設定できます。

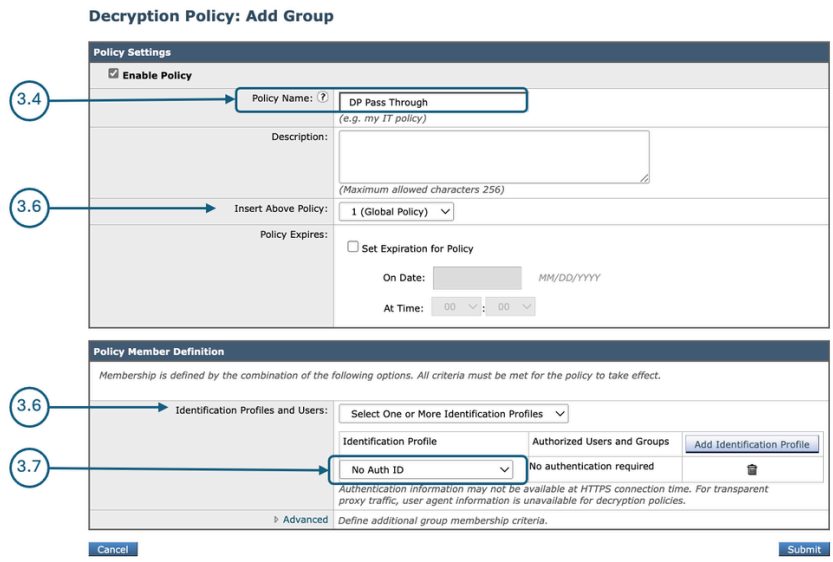
SWAでのパススルーの設定とトラフィックの許可

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
ステップ 1：URLのカスタムURLカテゴリを作成します。	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。

	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、このフィールドをブランクのままにして、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。

	 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 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。



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。

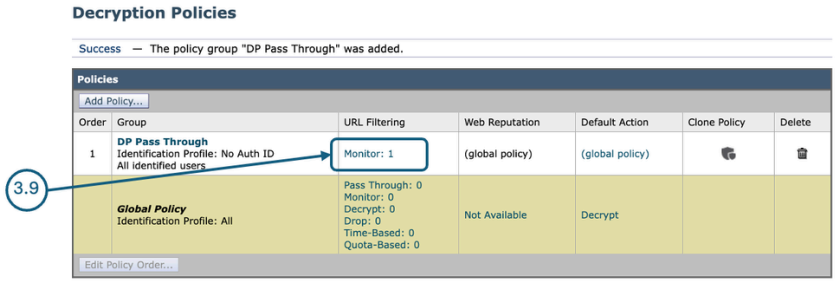
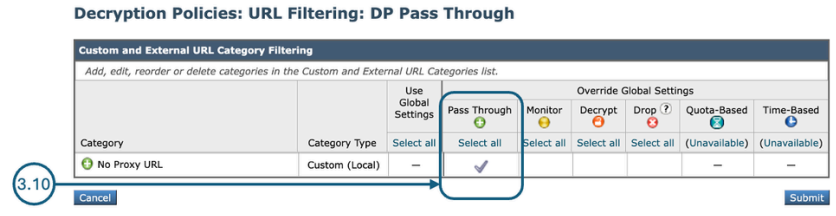


図 – URLフィルタリングの選択

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。



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。

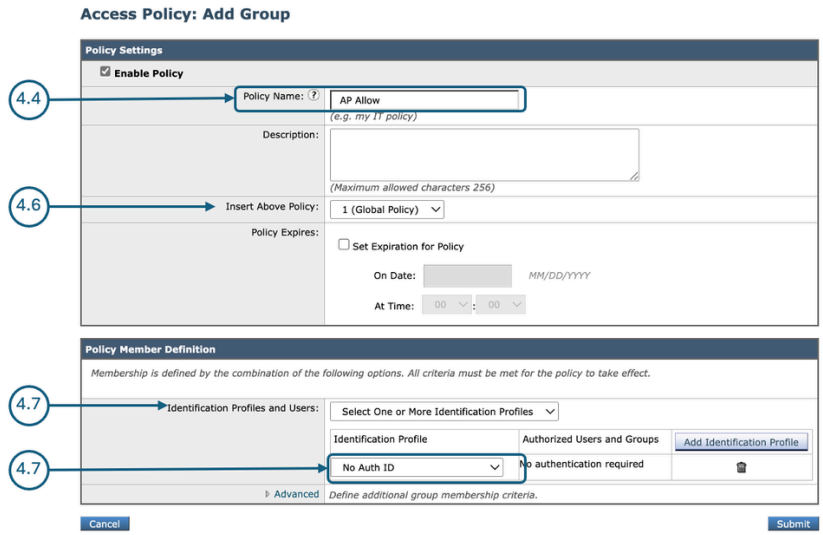
ステップ 4Microsoft Updatesトラフィックを許可するアクセスポリシーを作成します。	ステップ4.1:GUIから、Web Security Managerを選択し、Access Policyをクリックします。

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。



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。

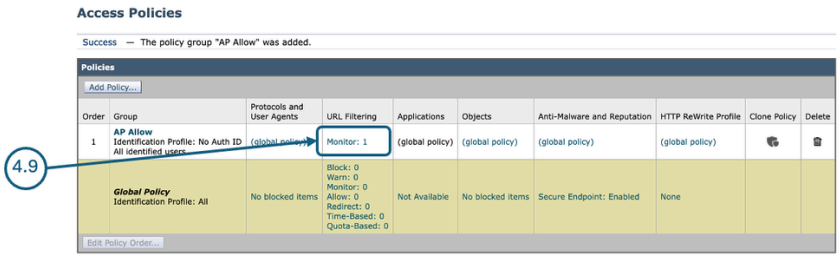
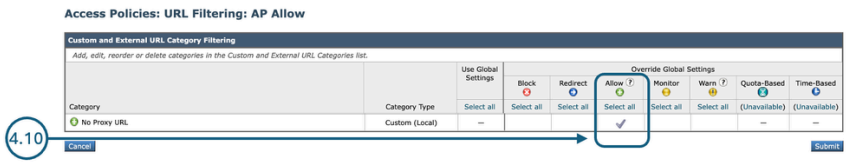


図 – URLフィルタリングの選択

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。



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。