

Bypass Traffic in Secure Web Appliance

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Different Types of Bypass](#)

[SWA Bypass Procedures by Deployment Type](#)

[Bypass Traffic in Explicit Deployment](#)

[PAC File Configuration](#)

[Browser Configuration \(Microsoft Edge, Internet Explorer, Google Chrome\)](#)

[Browser Configuration \(Mozilla FireFox\)](#)

[Browser Configuration \(Apple Safari\)](#)

[Group Policy Configuration](#)

[Bypass Traffic in TransparentDeployment](#)

[SWA Bypass Setting](#)

[Redirect the Traffic From WCCP/PBR Router](#)

[Configuring Pass Through and Allowing Traffic in SWA](#)

[Related Information](#)

Introduction

This document describes the steps to bypass traffic in Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SWA administration.
- Basic Networking and Proxy protocols

Cisco recommends that you have these tools installed:

- Physical or Virtual SWA
- Administrative Access to the SWA Graphical User Interface (GUI)

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Different Types of Bypass

In SWA, there are three different concepts of bypassing a traffic from reaching the SWA which depends on your Proxy deployment (Explicit or Transparent Deployment), or from being analyzed and scanned by the SWA. Here are a brief over view of these three concepts:

- **Bypass:** A setting that prevents traffic from reaching the SWA, which lowers Network Interface Card (NIC) utilization and removes the need for a session between the user and the appliance.
- **Pass Through:** This configuration prevents the SWA from decrypting HTTPS traffic. Despite this, the SWA continues to facilitate two distinct sessions: one between the client and the SWA, and a second between the SWA and the web server.
- **Allow:** A setting within the Access Policy where HTTP or decrypted traffic skips inspection by internal SWA engines, such as AMP, Sophos, WebRoot, and the Application Filter. In this case, still there are two sessions in use in the SWA.

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 ...

Image - Comparison Chart

SWA Bypass Procedures by Deployment Type

Bypass procedures vary depending on your proxy deployment model. Here is a brief overview of each type:

- **Explicit Deployment:** Clients are manually configured to direct traffic to the proxy.
- **Transparent Deployment:** Network infrastructure redirects traffic to the proxy automatically, requiring no client-side configuration.

Bypass Traffic in Explicit Deployment

To Bypass the Traffic in the Explicit Deployment, you must configure the Client to not forward the web request for the desired URLs to the SWA. As shown in this network diagram, some of the traffic are directly going to the Firewall or the Default Gateway to bypass the SWA (Path number 2).

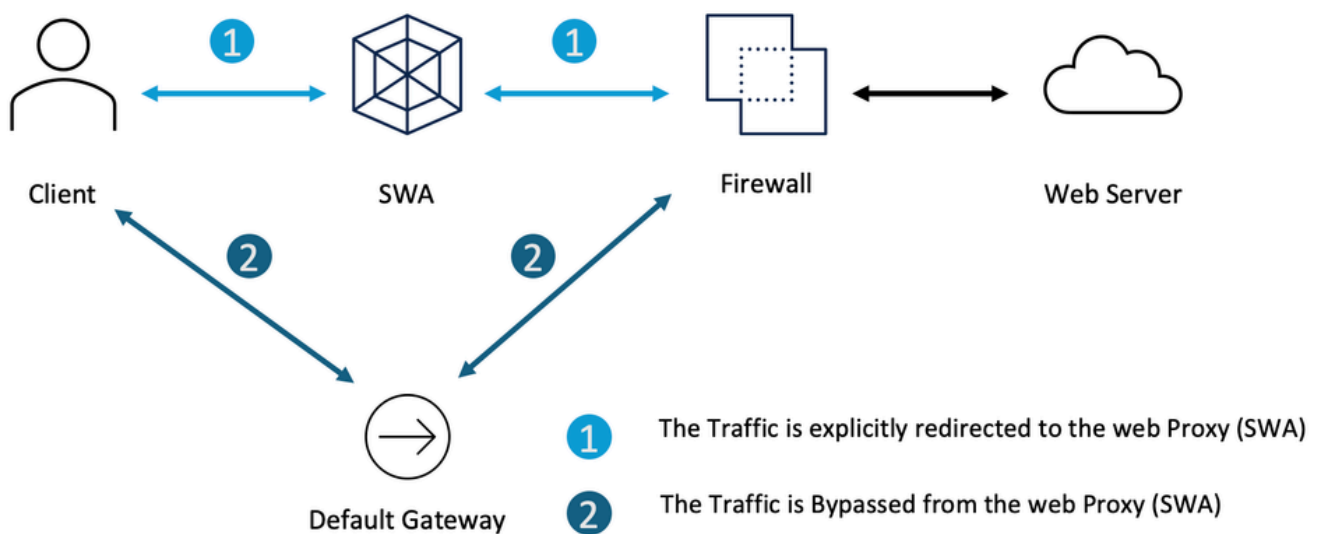



Image - Bypass the Traffic in Explicit Deployment

Depends on your explicit proxy deployment, you can exempt some URLs to redirected to the SWA.

Explicit Proxy Configuration	Steps to exclude URLs from reaching the SWA
PAC File Configuration	<p>Depends on how you configured your PAC file, you can define the exception list and set the action to DIRECT.</p> <p>Here are some samples to bypass the private IP address from reaching the SWA</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>This is an Example to Bypass the traffic to www.cisco.com from redirecting the SWA</p> <pre>if (localhostOrDomainIs(host, "www.cisco.com")) return "DIRECT";</pre> <p>This example is to bypass all the sub-domains of cisco.com from redirecting the SWA</p> <pre>if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";</pre> <hr/> <p> Note: Since PAC file is not Cisco product, the information is provided as a courtesy for your convenience. For further assistance, please contact the software vendor.</p> <hr/>
<p>Browser Configuration (Microsoft Edge, Internet Explorer, Google Chrome)</p>	<p>Step 1. In the Start Menu, type "Internet Options" and press enter</p> <p>Step 2. Navigate to Connections tab and click LAN Settings</p> <p>Step 3. Click on the Advanced</p> <p>Step 4. Define your desired URLs in the Exceptions section.</p>

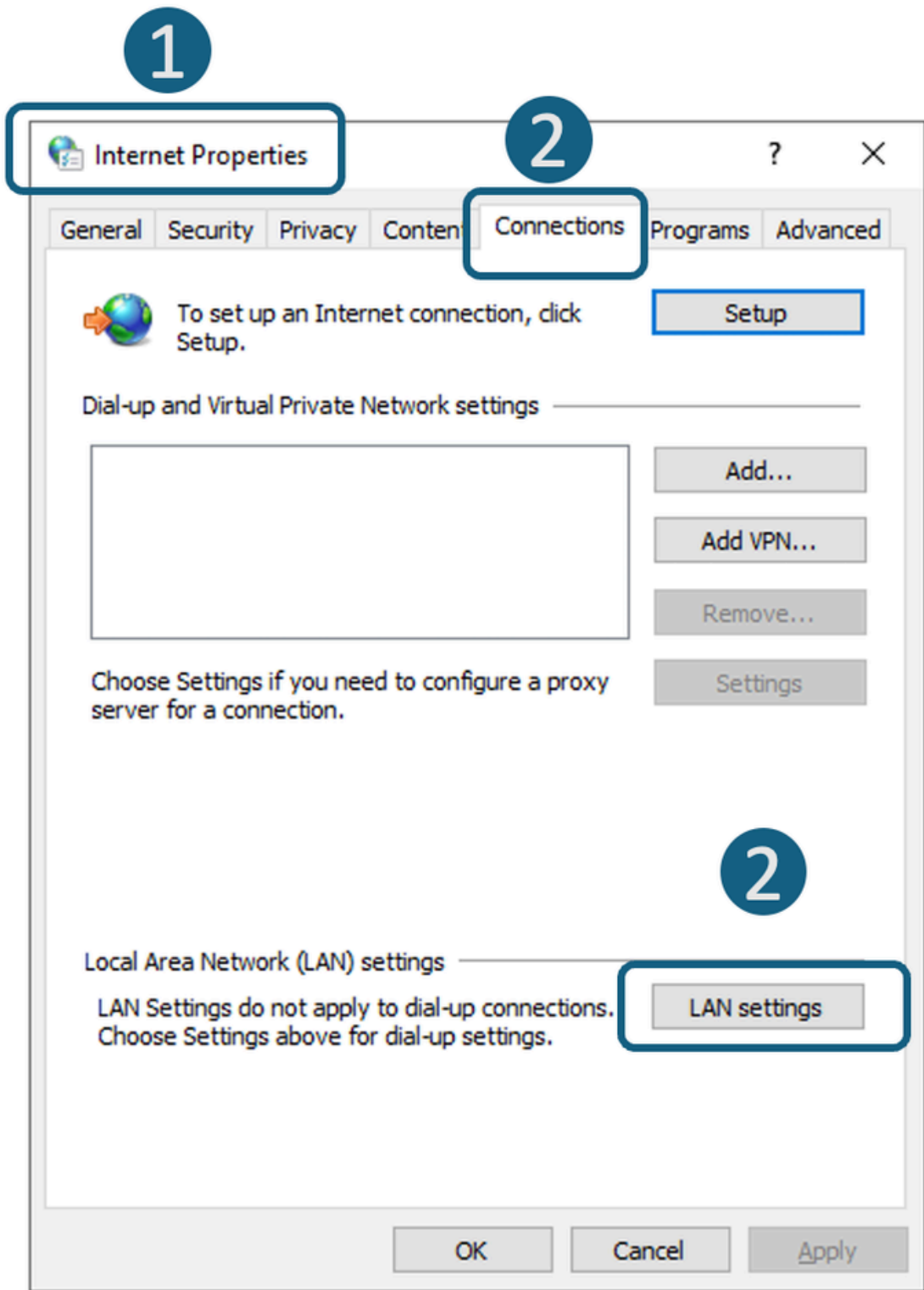
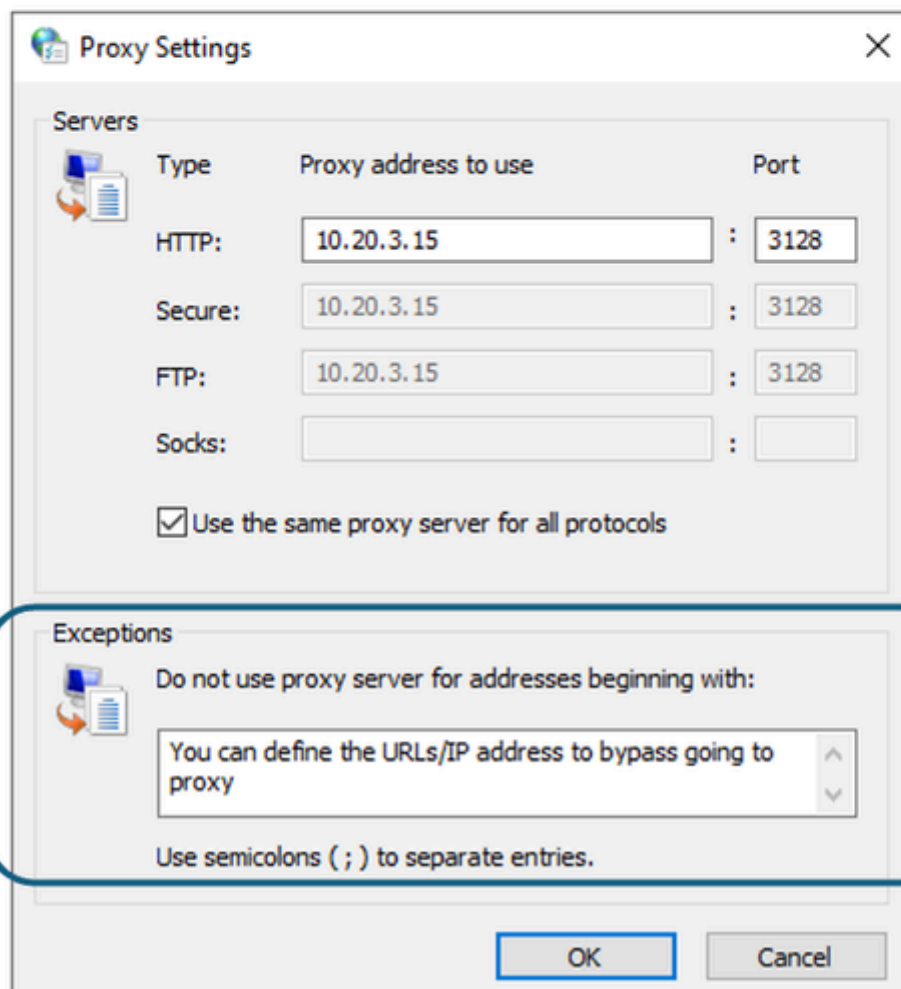
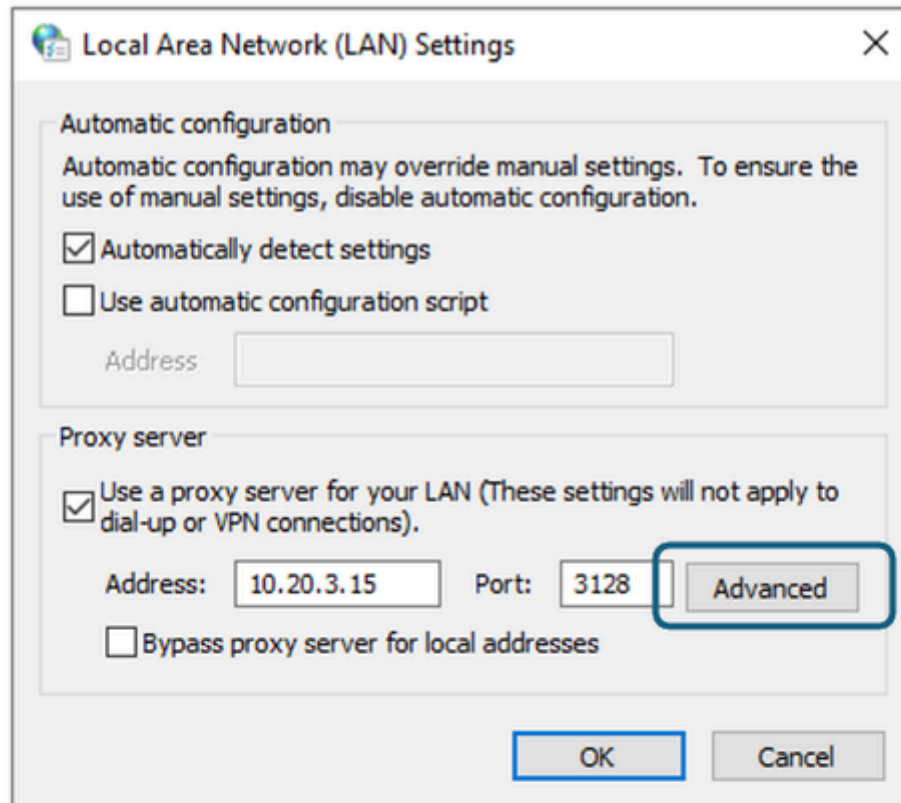


Image - Navigate to Lan Settings



Browser Configuration (Mozilla FireFox)

- Step 1.** On the top right corner, click on the three bar menu and select **Settings**.
- Step 2.** In the search bar, type **proxy**.
- Step 3.** Define your desired URLs in the **No Proxy for** section.

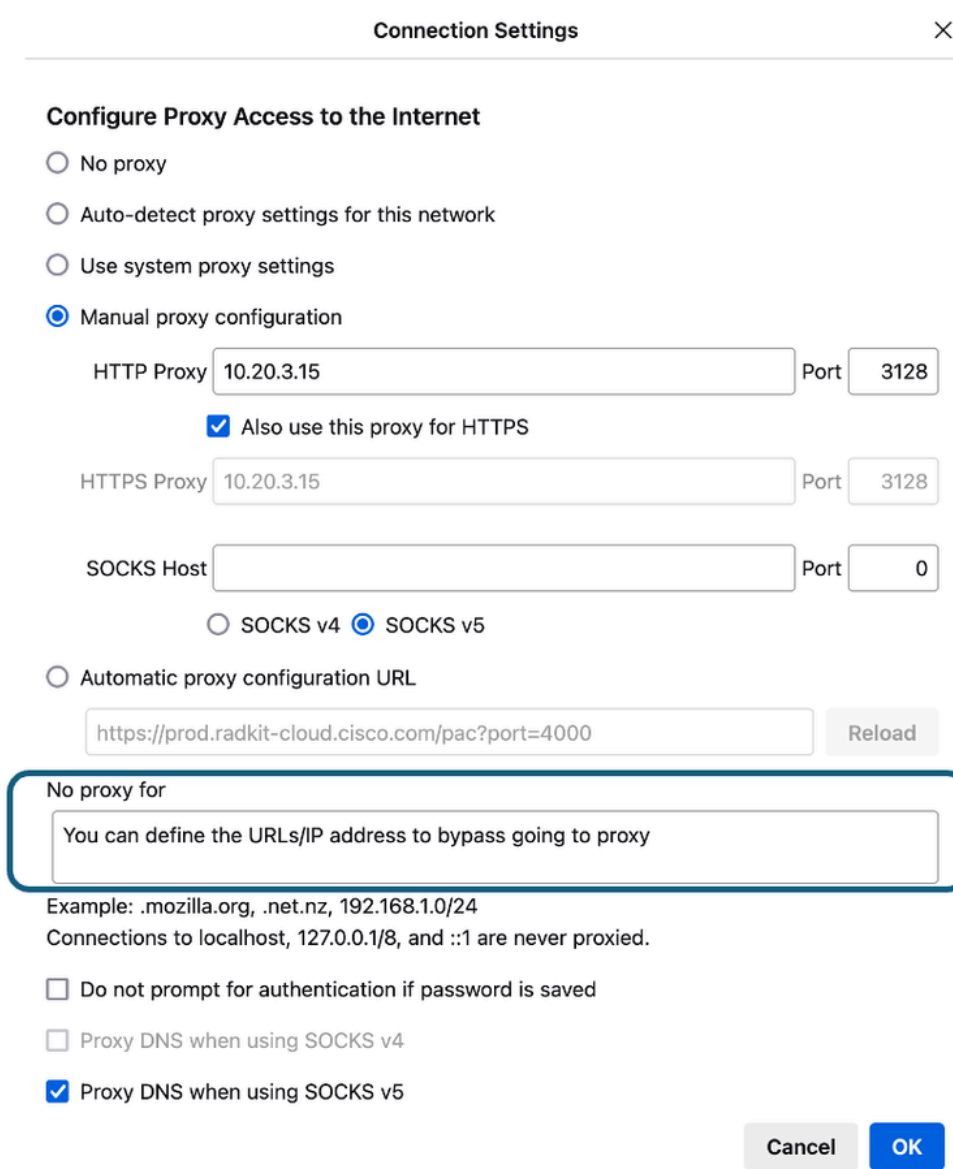


Image - Define the Exceptions in Fire Fox

Browser Configuration (Apple Safari)

- Step 1.** On the top-left corner, click on the Apple icon and choose **System Settings**.
- Step 2.** From the left panel navigate to **Network** and select the Network Interface you are using to access the Internet.
- Step 3.** Click on the **Details**.
- Step 4.** From the left panel, select **Proxies**.

Step 5. Define your desired URLs in the **Bypass Proxy Settings** section.

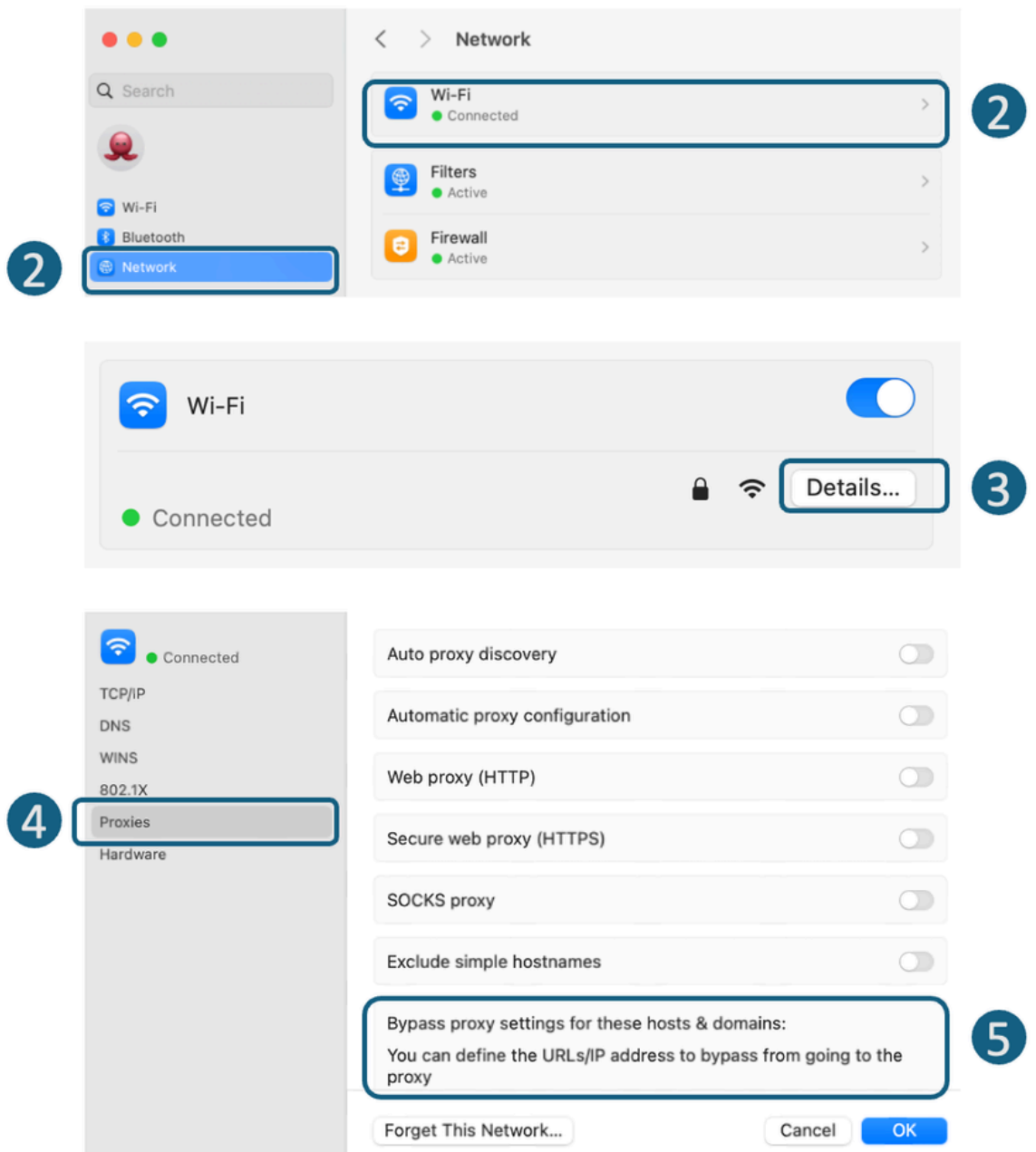


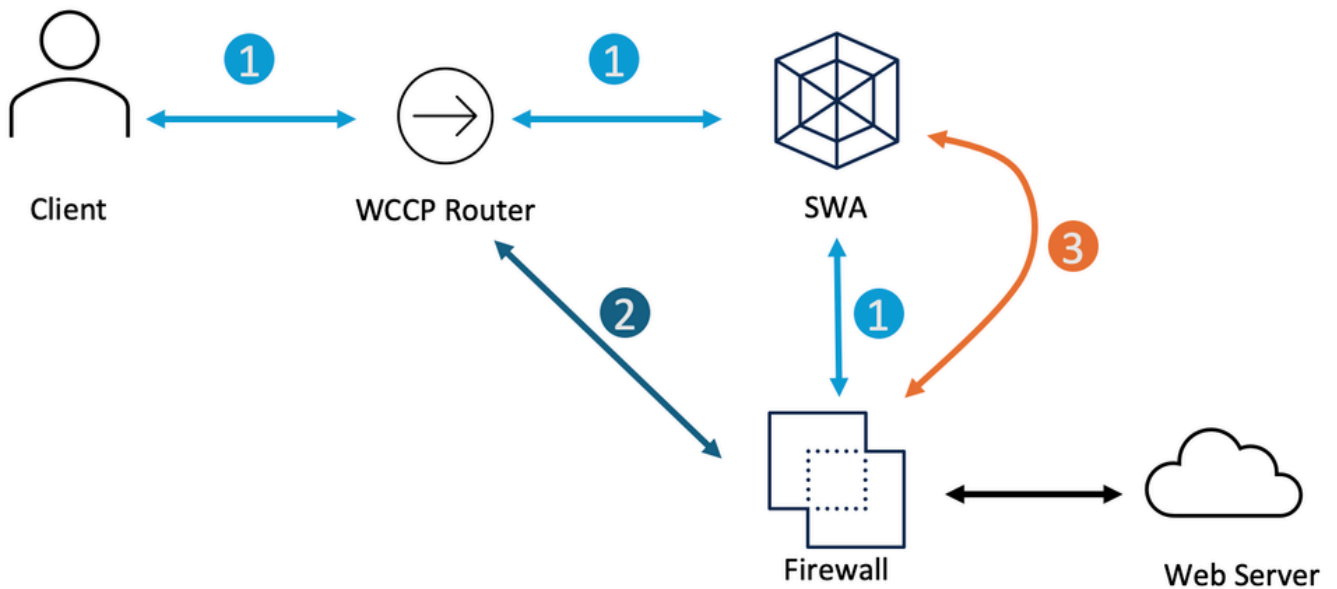
Image - Define the Exceptions in Fire Fox

Group Policy Configuration

Depends on how you configured the Group Policy to push the proxy settings, you can define the exception list.

Bypass Traffic in Transparent Deployment

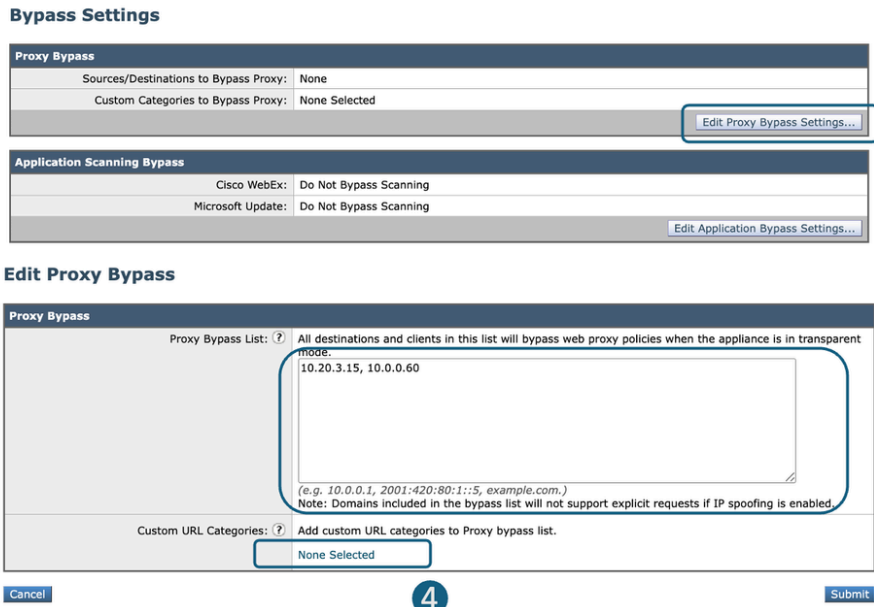
You can bypass traffic in a transparent deployment using either the WCCP router or SWA Bypass settings. SWA Bypass acts at Layer 3, routing traffic to the default gateway and bypassing the appliance entirely, which prevents processing and the creation of separate sessions.



- 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

Image - Bypass the Traffic in Transparent Deployment

<p>Bypassing traffic Transparent Proxy Deployment</p>	<p>Steps to bypass the traffic from reaching the SWA</p>
<p>SWA Bypass Setting</p>	<p>Step 1. From GUI, Choose Web Security Manager.</p> <p>Step 2. Select Bypass Settings.</p> <p>Step 3. Click Edit Proxy Bypass Settings.</p> <p>Step 4. You can enter the URL, IP address or adding a Custom URL Category to the list.</p> <p>Step 5. Submit and Commit the changes.</p>

	 <p>Bypass Settings</p> <p>Proxy Bypass</p> <p>Sources/Destinations to Bypass Proxy: None</p> <p>Custom Categories to Bypass Proxy: None Selected</p> <p>Application Scanning Bypass</p> <p>Cisco WebEx: Do Not Bypass Scanning</p> <p>Microsoft Update: Do Not Bypass Scanning</p> <p>Edit Proxy Bypass</p> <p>Proxy Bypass</p> <p>Proxy Bypass List: All destinations and clients in this list will bypass web proxy policies when the appliance is in transparent mode.</p> <p>10.20.3.15, 10.0.0.60</p> <p>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</p> <p>Note: Domains included in the bypass list will not support explicit requests if IP spoofing is enabled.</p> <p>Custom URL Categories: Add custom URL categories to Proxy bypass list.</p> <p>None Selected</p> <p>Cancel Submit</p> <p><i>Image - Configure Bypass Settings</i></p> <p>Tip: Traffic that is Bypassed with this settings are not logged in the Accesslogs and can be viewed in the Bypass_Logs.</p>
<p>Redirect the Traffic From WCCP/PBR Router</p>	<p>You can configure source or destination IP address in your WCCP or Policy Based Router (PBR) to not redirect some traffics to the SWA.</p>

Configuring Pass Through and Allowing Traffic in SWA

If the traffic is hitting the SWA and in order to reduce the load on the SWA to due to the privacy concerns you do not want the traffic for some URLs being inspected by the SWA, use these steps.

Steps	Steps
<p>Step 1. Create a Custom URL Category for the URLs.</p>	<p>Step 1.1. From GUI, Choose Web Security Manager and then click Custom and External URL Categories.</p> <p>Step 1.2. Click Add Category to add a Custom URL Category.</p> <p>Step 1.3. Assign a unique Category Name.</p> <p>Step 1.4. (Optional) Add Description.</p> <p>Step 1.5. From List Order, choose the first category to position on top.</p>

Step 1.6. From **Category** Typedrop-down list, choose **Local Custom Category**.

Step 1.7. Add desired URLs in the **Sites** Section.

Step 1.8. Submit.

Custom and External URL Categories: Add Category

The screenshot shows a web form titled "Edit Custom and External URL Category". The form has several sections: "Category Name" (text input with "No Proxy URL"), "Comments" (text area), "List Order" (text input with "1"), "Category Type" (dropdown menu with "Local Custom Category" selected), "Sites" (text area with "www.cisco.com" and a "Sort URLs" button), and "Advanced" (checkbox) with "Regular Expressions" (text area). Callouts 1.3 through 1.7 point to the Category Name, List Order, Category Type, and Sites fields respectively. A "Cancel" button is at the bottom left and a "Submit" button is at the bottom right.

Image - Create a Custom URL Category

Step 2. Create an Identification Profile to exempt traffic from Authentication.

Step 2.1. From GUI, Choose **Web Security Manager** and then click **Identification Profiles**.

Step 2.2. Click **Add Profile** to add a profile.

Step 2.3. Use the **Enable Identification Profile** check box to enable this profile, or to quickly disable it without deleting it.

Step 2.4. Assign a unique profile **Name**.

Step 2.5. (Optional) Add **Description**.

Step 2.6. From the **Insert Above** drop-down list, choose where this profile is to appear in the table.

Step 2.7. In the **User Identification Method** section, choose **Exempt from authentication/ identification**.

Step 2.8. In the **Define Members by Subnet**, leave this field blank to include all Client IP address unless you would like to Pass Through the traffic for a certain IP addresses.

Step 2.9. From **Advanced** section, choose **Custom URL Categories**.

Identification Profiles: Add Profile

The screenshot shows the 'Client / User Identification Profile Settings' form. It is divided into three main sections: 'Enable Identification Profile', 'User Identification Method', and 'Membership Definition'. Callout 2.4 points to the 'Name' field, which contains 'No Auth ID'. Callout 2.6 points to the 'Insert Above' dropdown menu, which is set to '1 (Global Profile)'. Callout 2.7 points to the 'Identification and Authentication' dropdown, which is set to 'Exempt from authentication / Identification'. Callout 2.9 points to the 'Advanced' options in the 'Membership Definition' section, specifically the 'URL Categories' dropdown, which is set to 'None Selected'. The 'Advanced' section also includes 'Proxy Ports' and 'User Agents', both set to 'None Selected'. The form has 'Cancel' and 'Submit' buttons at the bottom.

Image - Add Identification Profile

Step 2.10. Add the Custom URL Category that was created on Step 1.

Step 2.11. Click Done.

Step 2.12. Submit.

Step 3. Create a Decryption Policy to pass through traffic.

Step 3.1. From GUI, Choose **Web Security Manager** and then click **Decryption Policy**.

Step 3.2. Click **Add Policy** to add a Decryption Policy.

Step 3.3. Use the **Enable Policy** check box to enable this policy.

Step 3.4. Assign a unique Policy **Name**.

Step 3.5. (Optional) Add **Description**.

Step 3.6. From the **Insert Above Policy** drop-down list, choose the first Policy.

Step 3.7. From the **Identification Profiles and Users**, choose the Identification Profile that you created in **Step 2**.

Step 3.8. Submit.

Decryption Policy: Add Group

Policy Settings

Enable Policy

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

Description:
(Maximum allowed characters 256)

Insert Above Policy:

Policy Expires:

Set Expiration for Policy

On Date:

At Time:

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:

Define additional group membership criteria.

Image - Create a Decryption Policy

Step 3.9. In the **Decryption Policies** page, under **URL Filtering**, click on the link associated with this new Decryption Policy.

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)	<input type="button" value="Clone"/>	<input type="button" value="Delete"/>
	Global Policy Identification Profile: All	Pass Through: 0 Monitor: 0 Decrypt: 0 Drop: 0 Time-Based: 0 Quota-Based: 0	Not Available	Decrypt		

Image - Select URL Filtering

Step 3.10. Select **Pass Through** as the action for the URL Category created on **Step 1**.

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	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop ?	Quota-Based	Time-Based
<input checked="" type="checkbox"/> No Proxy URL	Custom (Local)	Select all	<input checked="" type="text" value="Select all"/>	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Image - Set the Action to Pass Through

Step 3.11. Submit.

Step 4. Create an Access Policy to

Step 4.1. From GUI, Choose **Web Security Manager** and then

allow Microsoft Updates traffic.

click **Access Policy**.

Step 4.2. Click **Add Policy** to add an Access Policy.

Step 4.3. Use the **Enable Policy** check box to enable this policy.

Step 4.4. Assign a unique **Policy Name**.

Step 4.5. (Optional) Add **Description**.

Step 4.6. From the **Insert Above Policy** drop-down list, choose the first Policy.

Step 4.7. From the **Identification Profiles and Users**, choose the Identification Profile that you created in Step 2.

Step 4.8. **Submit**.

Access Policy: Add Group

Policy Settings

Enable Policy

Policy Name: (e.g. my 11 policy)

Description:

(Maximum allowed characters 256)

Insert Above Policy:

Policy Expires: Set Expiration for Policy

On Date:

At Time:

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
<input type="text" value="No Auth ID"/>	No authentication required	<input type="button" value="Add Identification Profile"/>

Image - Create Access Policy

Step 4.9. On the **Access Policies** page, under **URL Filtering**, click on the link associated with this new Access Policy.

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)	<input type="button" value="Clone"/>	<input type="button" value="Delete"/>
	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		

Image - Select URL Filtering

Step 4.10. Select **Allow** as the action for the Custom URL category created for the URL Category created on Step 1.

Access Policies: URL Filtering: AP Allow

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	Override Global Settings						
			Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based
<input checked="" type="checkbox"/> No Proxy URL	Custom (Local)	--	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Image - Set the Action to Allow

Step 4.11. Submit.

Step 4.12. Commit changes.

Related Information

- [Bypass Microsoft Updates Traffic in Secure Web Appliance](#)
- [Bypass Authentication in Secure Web Appliance - Cisco](#)
- [User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - GD\(General Deployment\) - Classify End-Users for Policy Application \[Cisco Secure Web Appliance\] - Cisco](#)
- [Configure Custom URL Categories in Secure Web Appliance - Cisco](#)
- [How To Exempt Office 365 Traffic From Authentication and Decryption on Cisco Web Security Appliance \(WSA\) - Cisco](#)
- [Use Secure Web Appliance Best Practices - Cisco](#)
- [Block Traffic in Secure Web Appliance](#)
- [Block Upload Traffic in Secure Web Appliance](#)
- [Block Executable File Download in SWA](#)