Bypass Traffic in Secure Web Appliance

Contents

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).

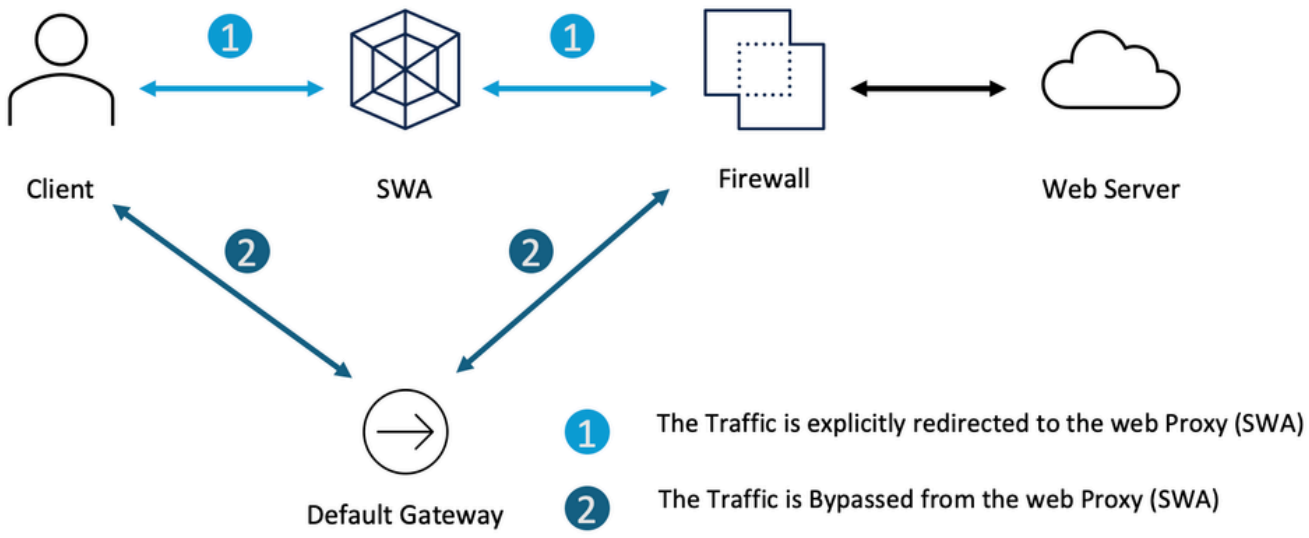


Image - Bypass the Traffic in Explicit Deployment

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	Depends on how you configured your PAC file, you can define the exception list and set the action to **DIRECT.**
	
	Here are some samples to bypass the private IP address from reaching the SWA
	
	`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";`

	This is an Example to Bypass the traffic to www.cisco.com from redirecting the SWA
	
	`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`
	
	This example is to bypass all the sub-domains of cisco.com from redirecting the SWA
	
	`if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";`
	
	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.

Browser Configuration (Microsoft Edge, Internet Explorer, Google Chrome)	**Step 1.** In the Start Menu, type "**Internet Options**" and press enter **Step 2.** Navigate to **Connections** tab and click **LAN Settings** **Step 3.** Click on the **Advanced** **Step 4.** Define your desired URLs in the **Exceptions** section.

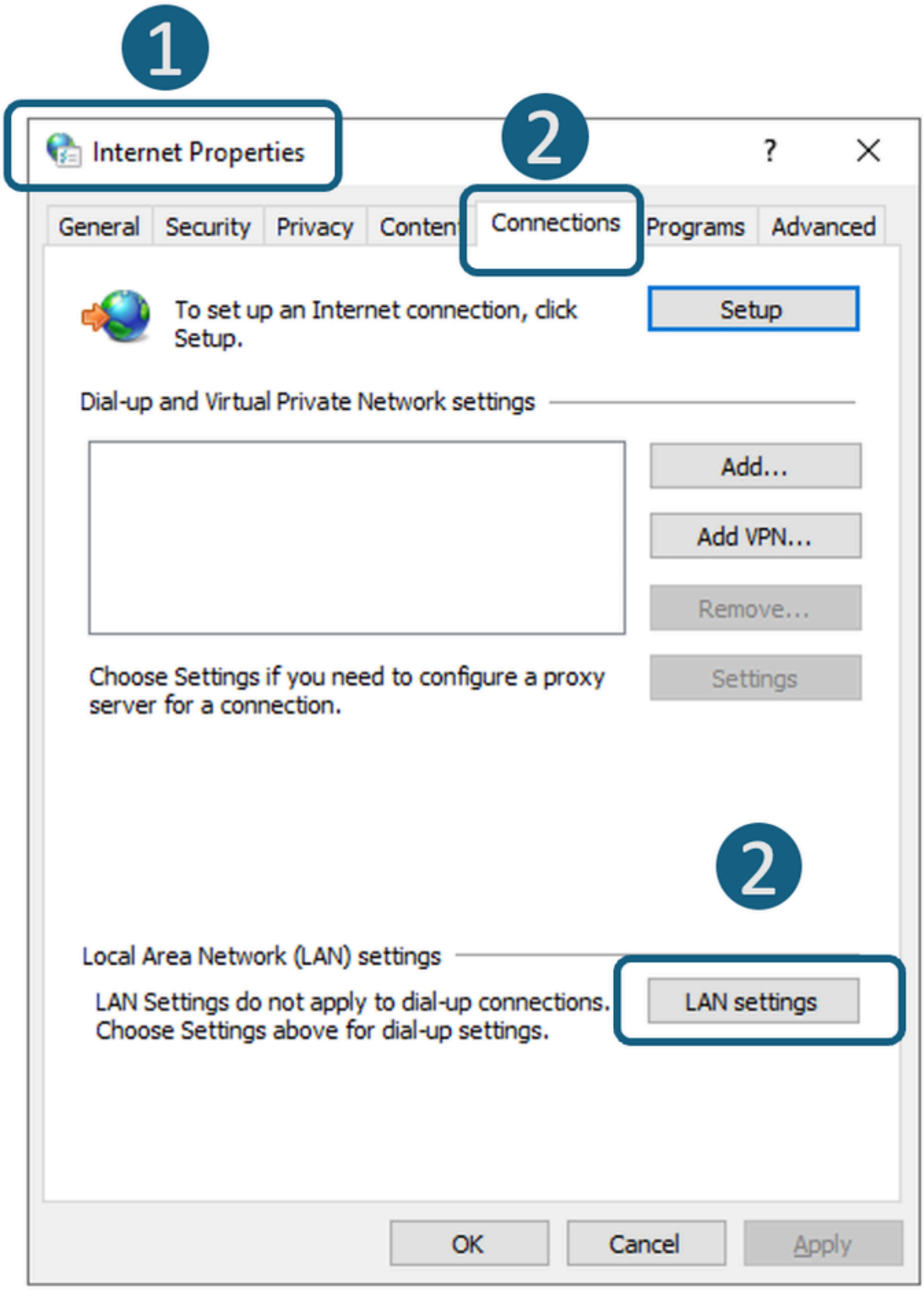


Image - Navigate to Lan Settings

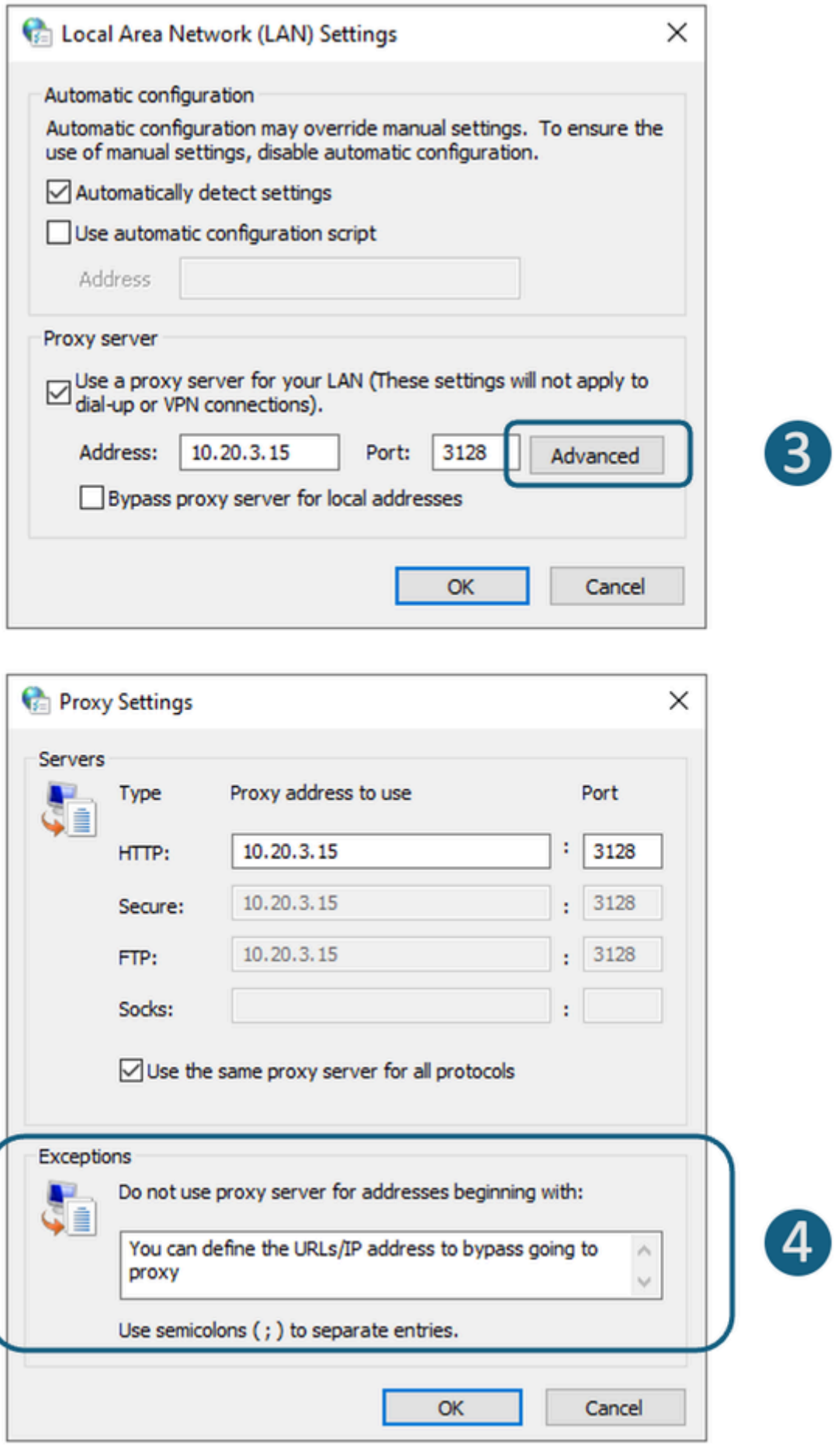
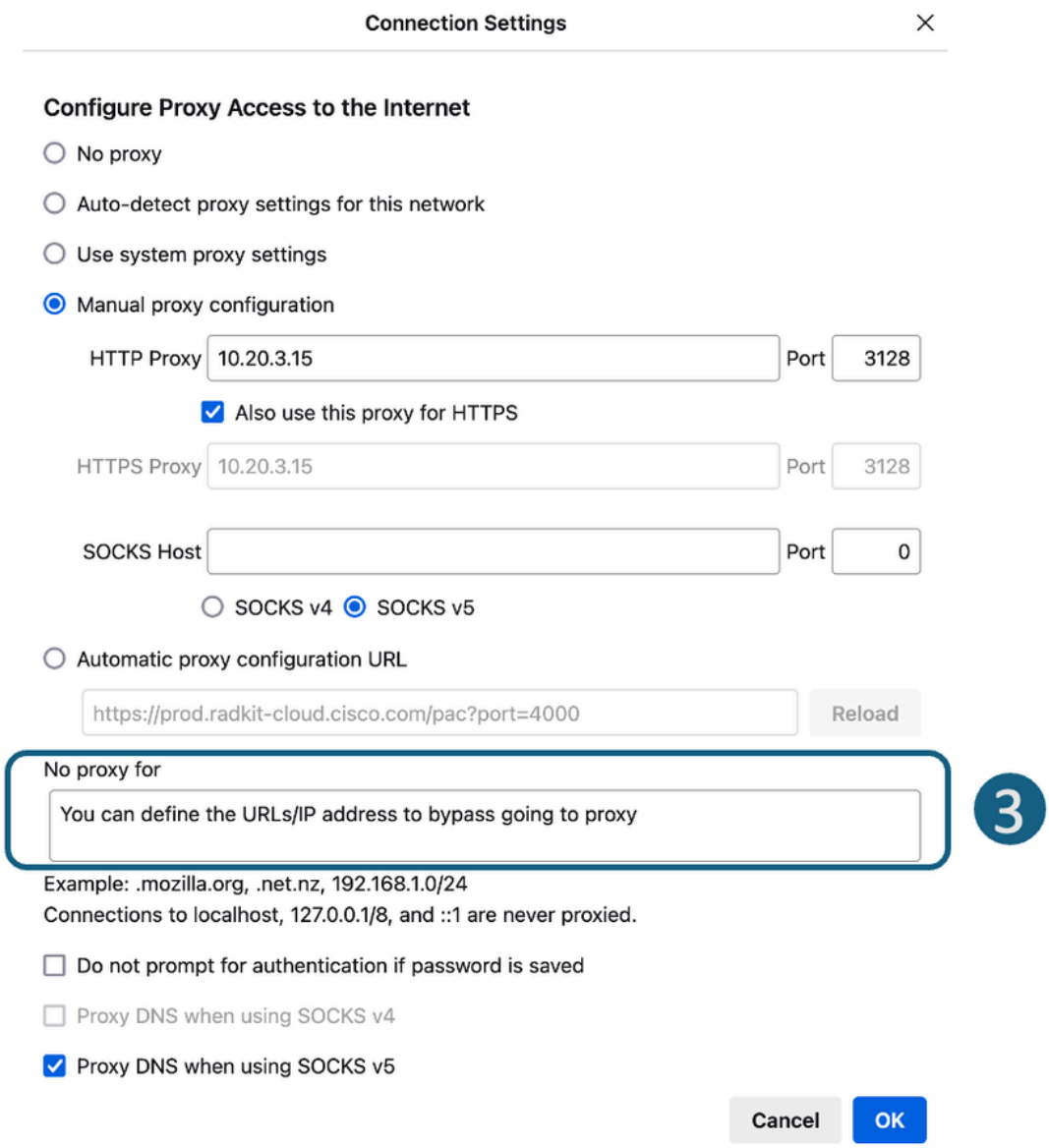
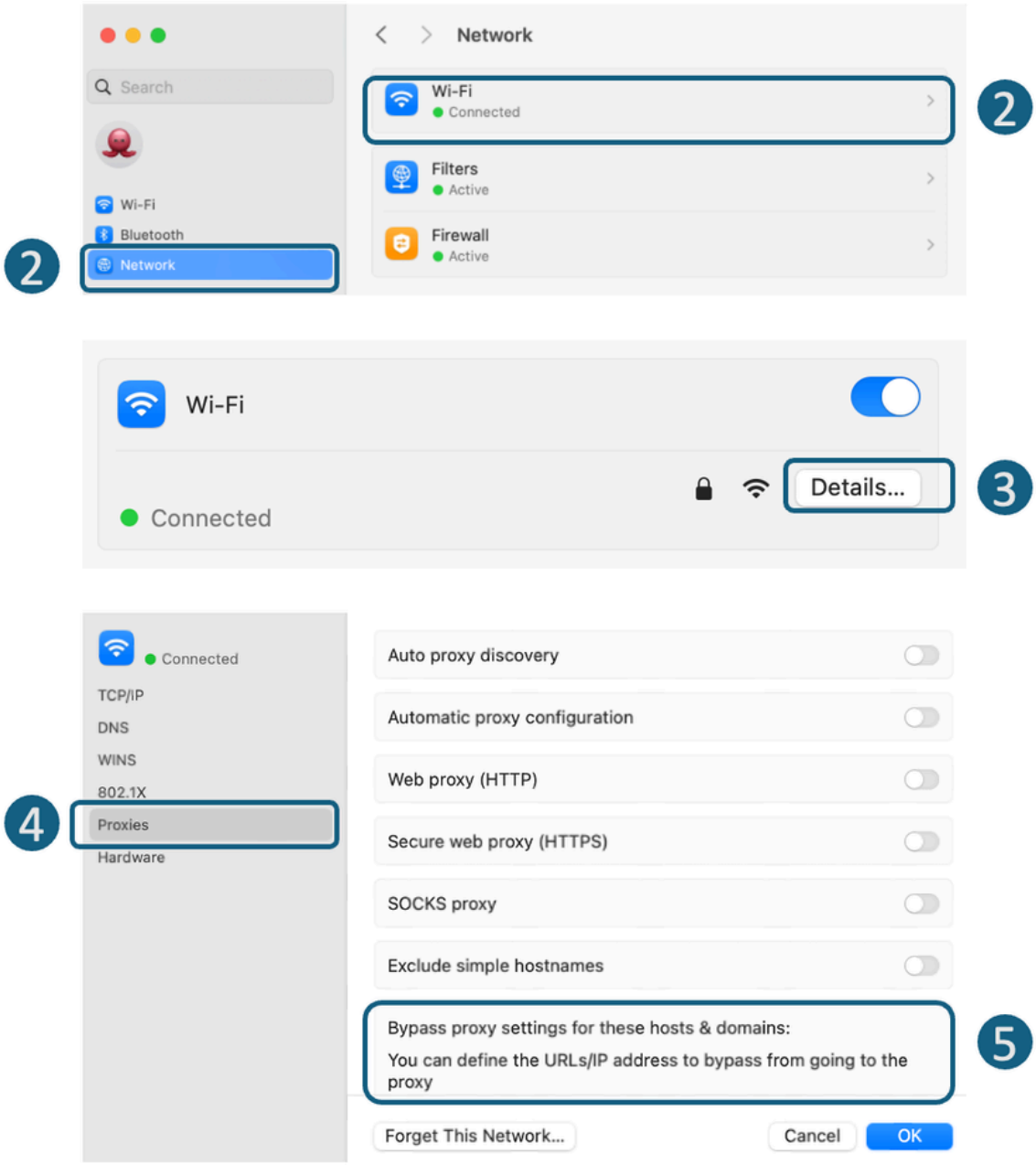


Image - Define the Exceptions

Browser Configuration (Mozila 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.

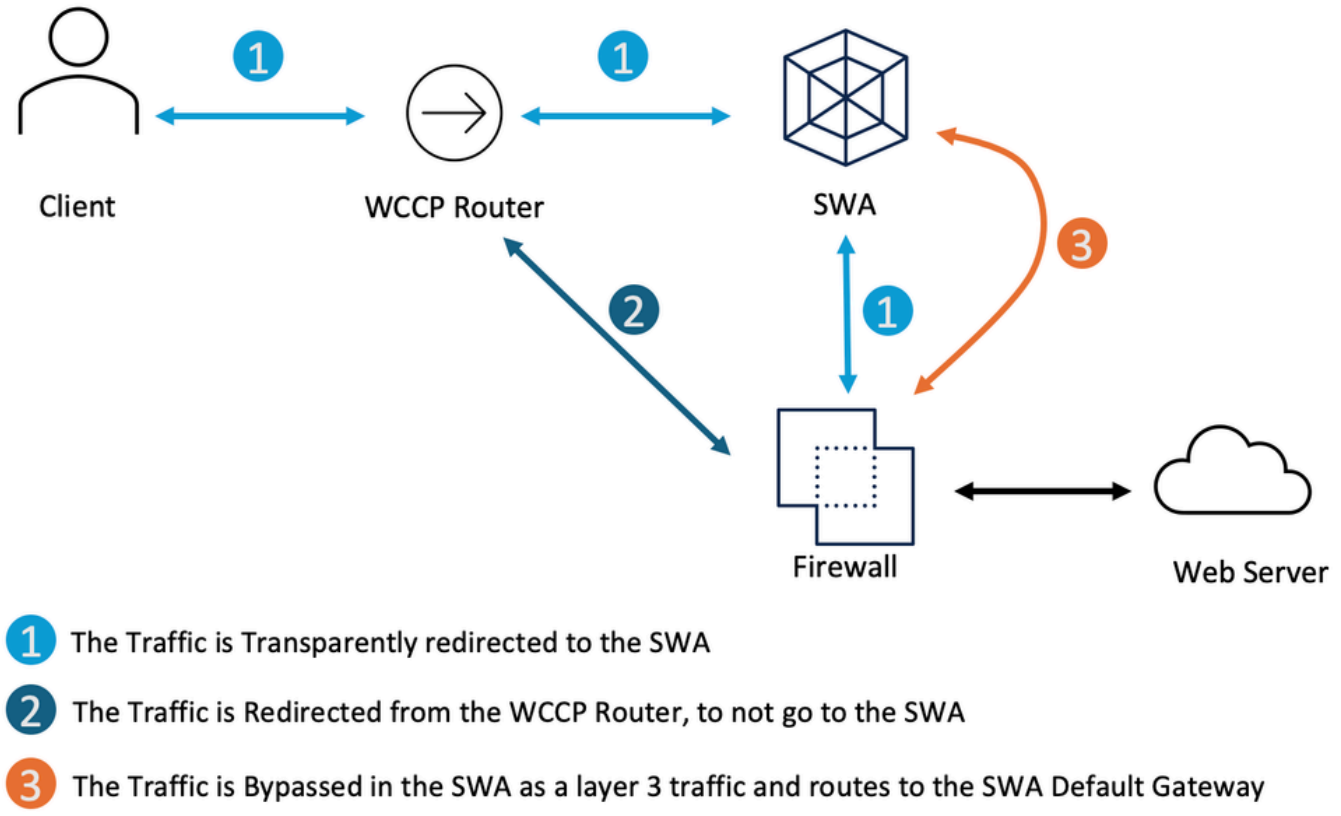
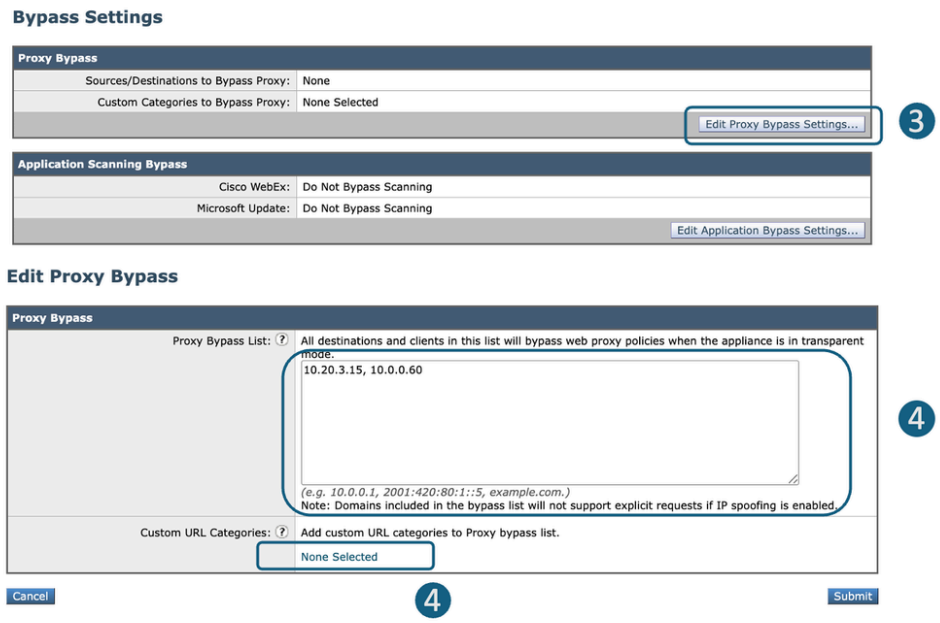


Image - Bypass the Traffic in Transparent Deployment

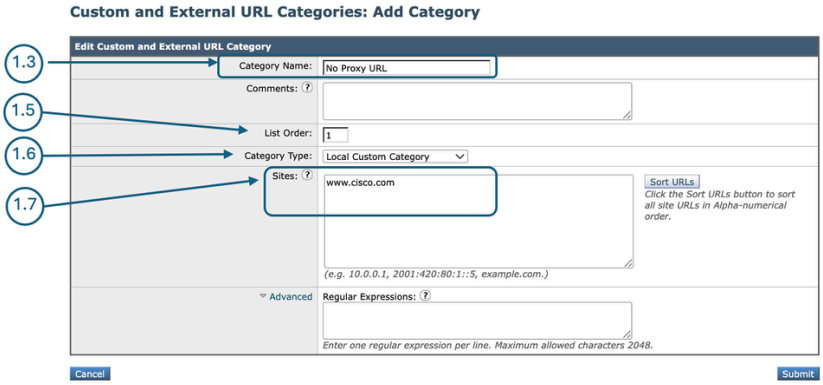
Bypassing traffic Transparent Proxy Deployment	**Steps to bypass the traffic from reaching the SWA**
SWA Bypass Setting	**Step 1.** From **GUI**, Choose **Web Security Manager**. **Step 2.** Select **Bypass Settings**. **Step 3.** Click **Edit Proxy Bypass Settings**. **Step 4.** You can enter the URL,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

	 *Image - Configure Bypass Settings* **Tip**: Traffic that is Bypassed with this settings are not logged in the Accesslogs and can be viewed in the Bypass_Logs.
Redirect the Traffic From WCCP/PBR Router	You can configure source or destination IP address in your WCCP or Policy Based Router (PBR) to not redirect some traffics to the SWA.

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

	Step 1.6. From **Category Type**drop-down list, choose **Local Custom Category.** **Step 1.7.** Add desiered URLs in the **Sites** Section. **Step 1.8. Submit**.  *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**.

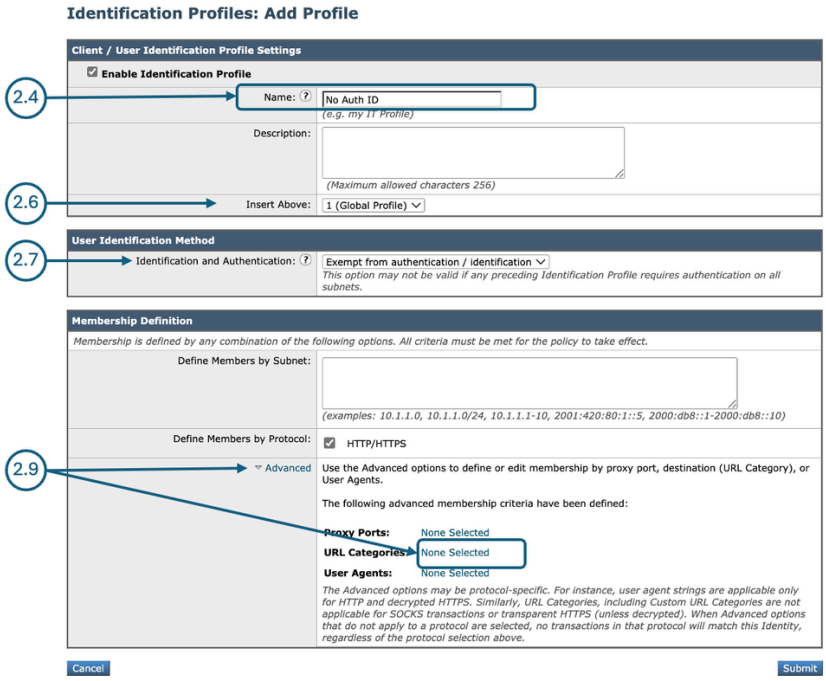


Image - Add Identification Profile

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.

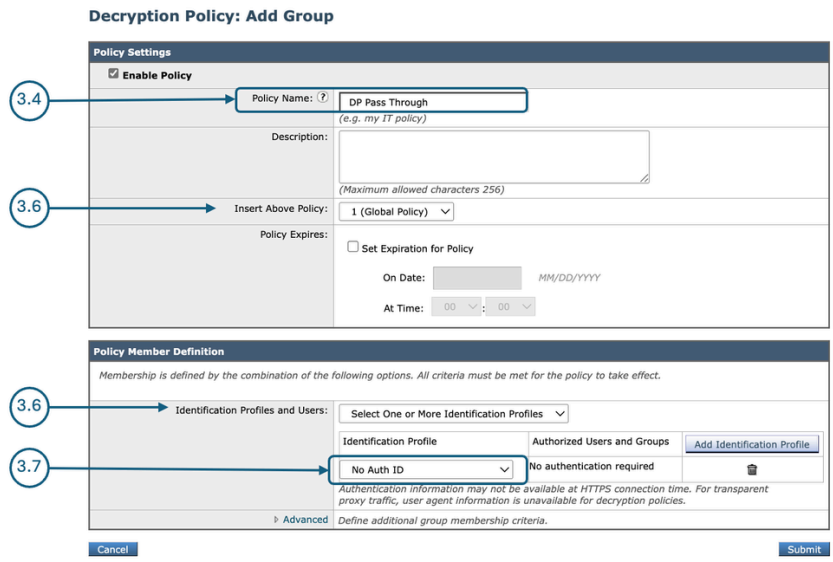


Image - Create a Decryption Policy

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

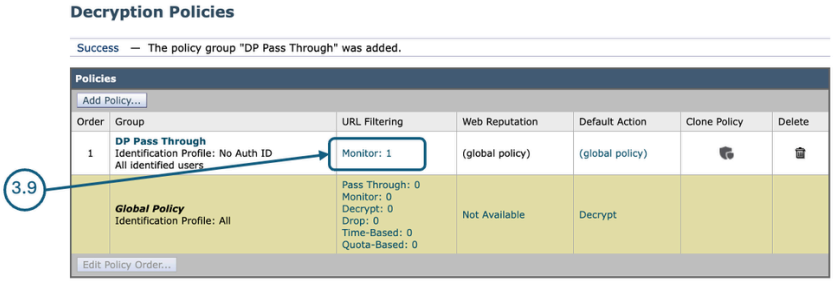


Image - Select URL Filtering

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

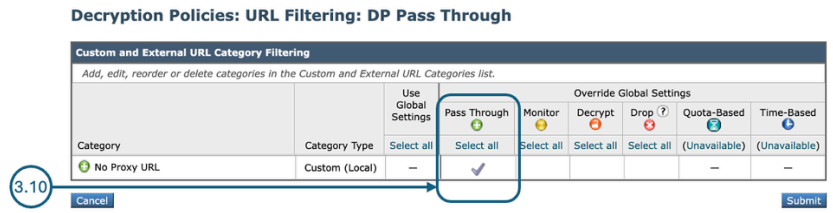


Image - Set the Action to Pass Through

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.

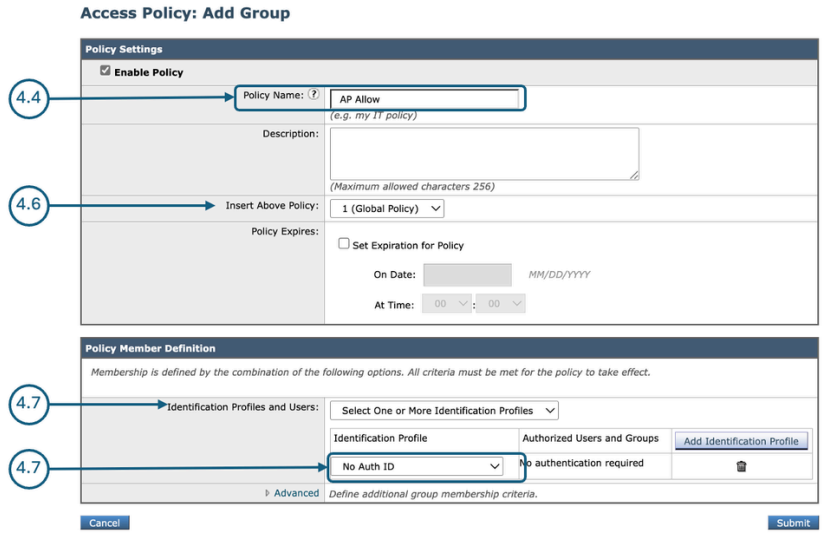


Image - Create Access Policy

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

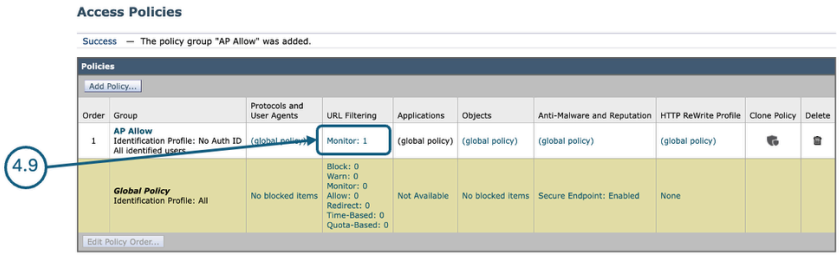


Image - Select URL Filtering

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

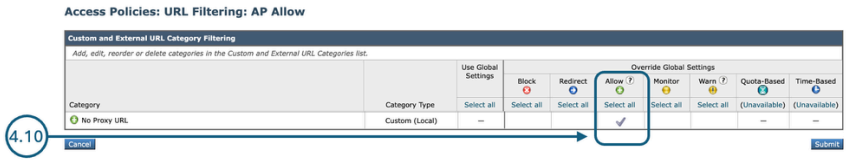


	Image - Set the Action to Allow **Step 4.11. Submit**. **Step 4.12. Commit** changes**.**

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