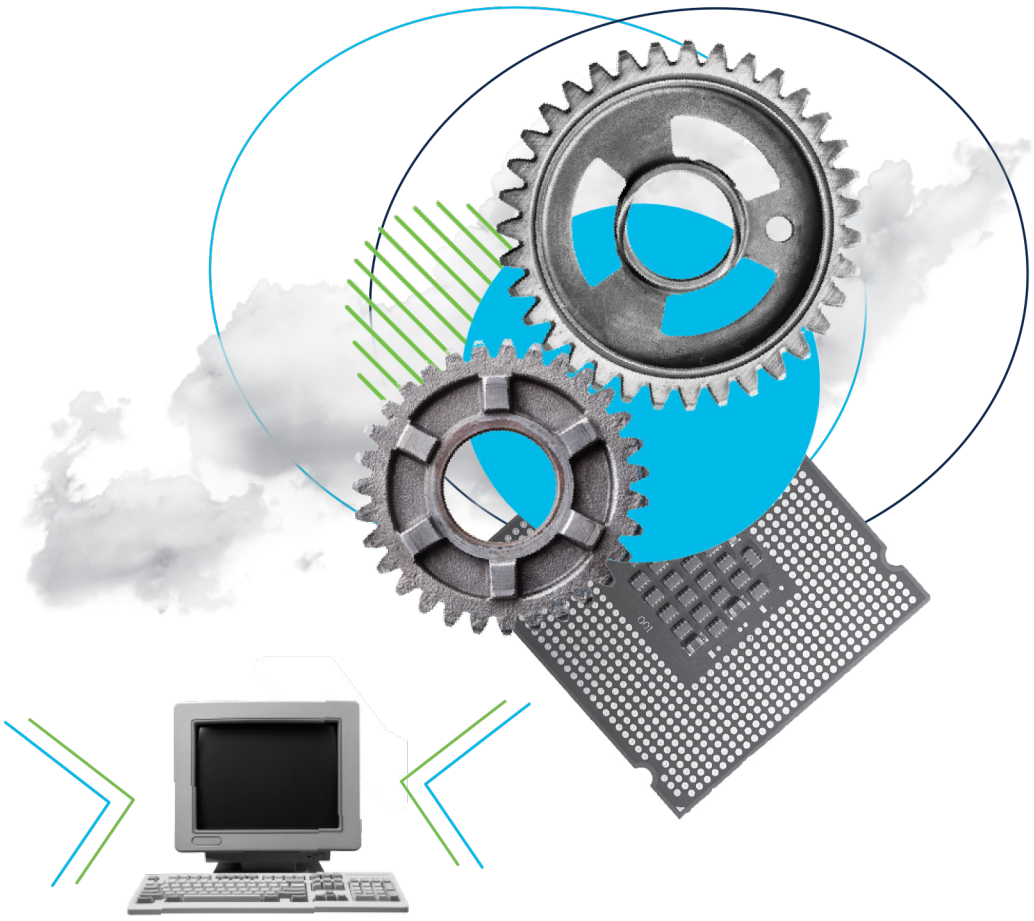
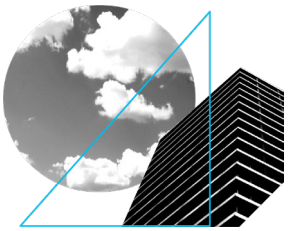
CISCO
SECURE

Isolate with Secure Web Appliance



Contents



Overview

The ever-changing cyberthreat landscape makes it increasingly challenging to ensure that zero attacks, zero malware, and zero infections affect your organization. Providing complete security means minimizing the number of attacks, malware, and infections and their impact on your organization by enabling the market's best-in-class features available within the Cisco® Secure Web Appliance.

Users' expectations when accessing information have also changed considerably where speed, efficiency, and efficacy are the critical requirements. Fast web browsing is expected to occur, whether the user is connected through a LAN, wireless network, satellite, or mobile network connection. Accessibility and faster speed mean more inspections are required on web traffic. Therefore, integrating multiple web security technologies ensures web traffic inspection efficiency to block attacks and malware and prevent infections from propagating through your network.

Introduction to browser isolation technology

Browser isolation technology provides an added layer of security that isolates any browser-based web traffic to ensure that no web activity is executed locally within a user's browser—hence eliminating any malware, attack, or infection from being executed within a user's local network and infrastructure.

This document discusses enabling the Remote Browser Isolation (RBI) solution in Secure Web Appliance to ensure that any malware or attacks that can be stopped locally by the Secure Web Appliance will be detected, in the cloud, away from the customer's network and the end user's machine.

"Almost all successful attacks on users originate from the public internet, and many involve web-based attacks. Security and risk management leaders can contain damage by using remote browser isolation to separate end-user internet browsing sessions from enterprise endpoints and networks."

– Gartner, Innovation Insight for Remote Browser Isolation, 2018

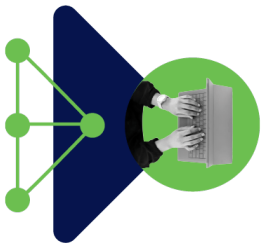
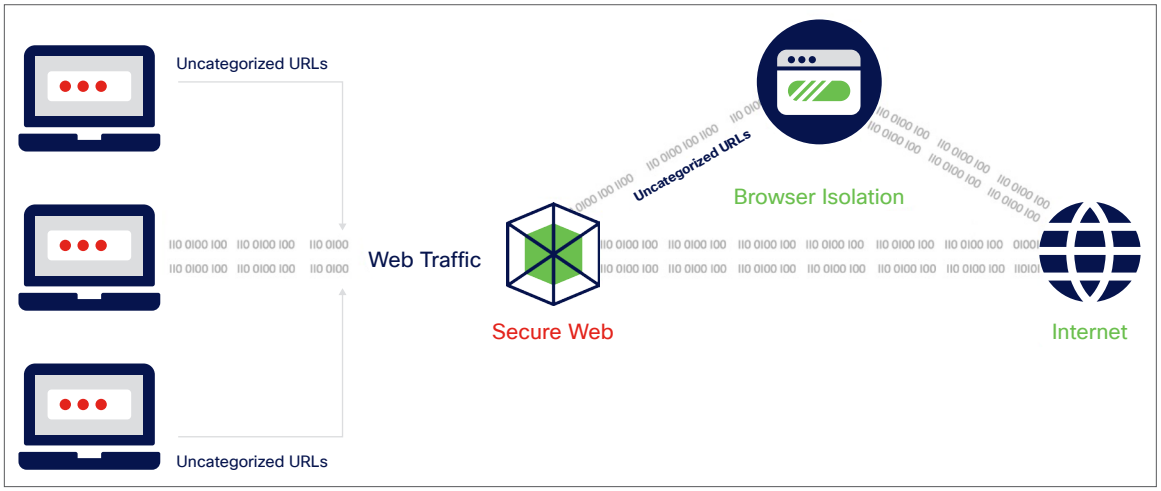


Figure 1. Browser isolation with Secure Web Appliance



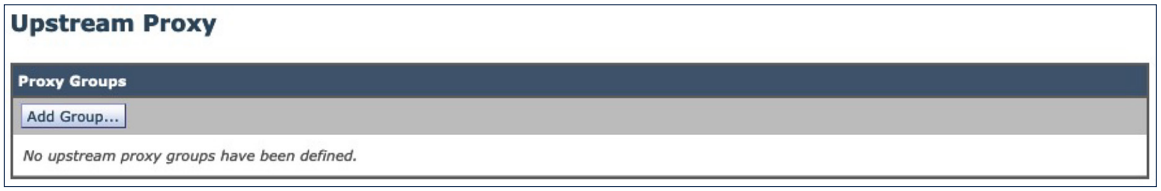
Product requirements

- Secure Web Appliance (support for all hardware and virtual platforms)
- Remote Browser Isolation license

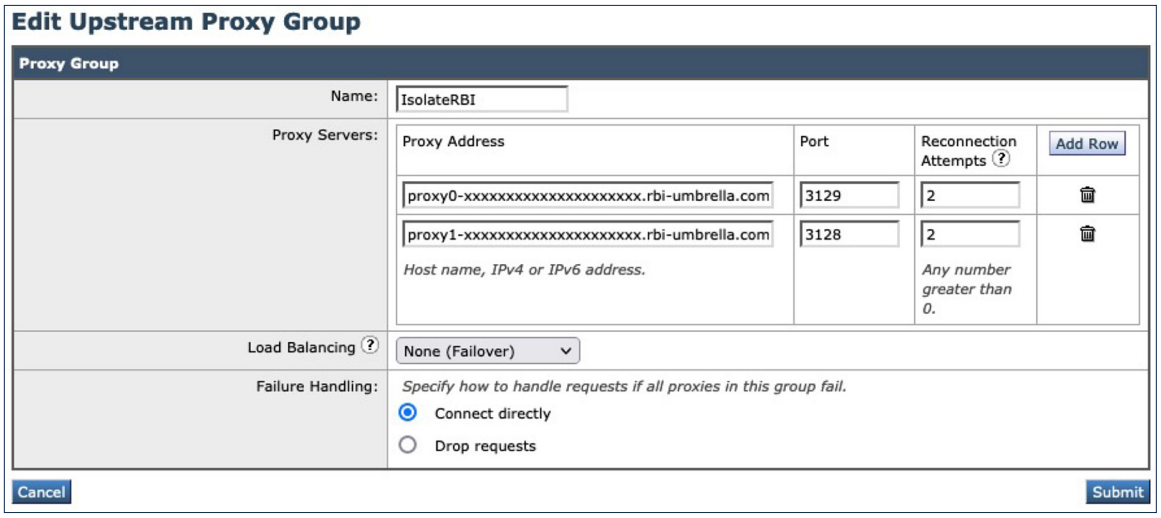
Configuration

Step 1 – Log in to the Secure Web Appliance UI using the admin credential: https://wsa_hostname:8443.

Step 2 – Navigate to **Network > Upstream Proxy,** and click on the **Add Group** button:

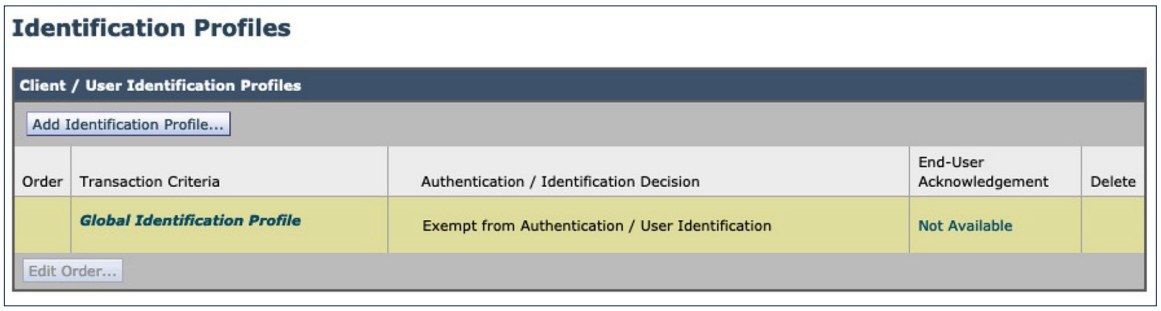


Step 3 – Configure the upstream proxy's name and the remote browser isolation server FQDNs. Click the **Submit** button to save the configuration.



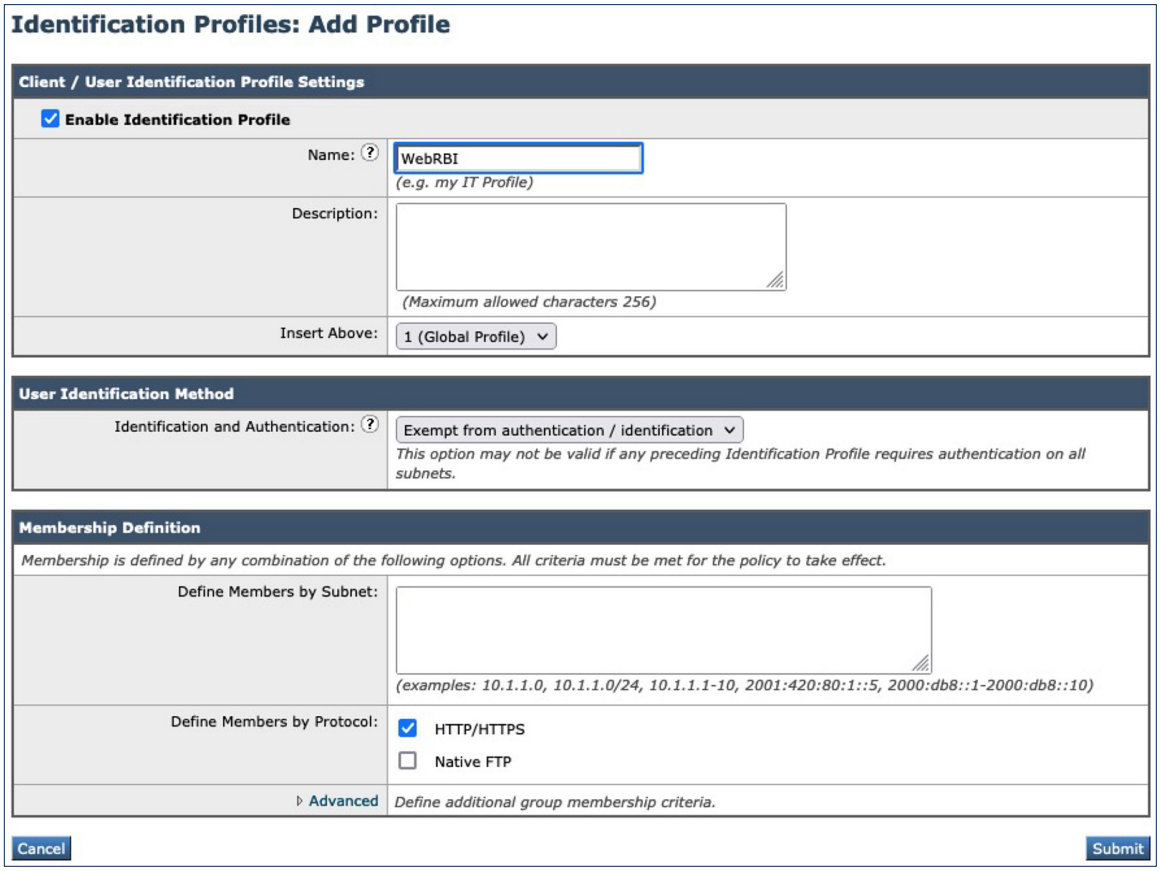
Step 4 – Create the identification profile to determine the web traffic selectively proxied from Secure Web Appliance to Remote Browser Isolation Security.

Navigate to **Web Security Manager > Identification Profiles,** and click on the **Add Identification Profile** button:



Step 5 – Configure a placeholder for web traffic identification to be an upstream proxy for RBI Security. The following section discusses different use cases in which configuration can easily be modified on the identification profile.

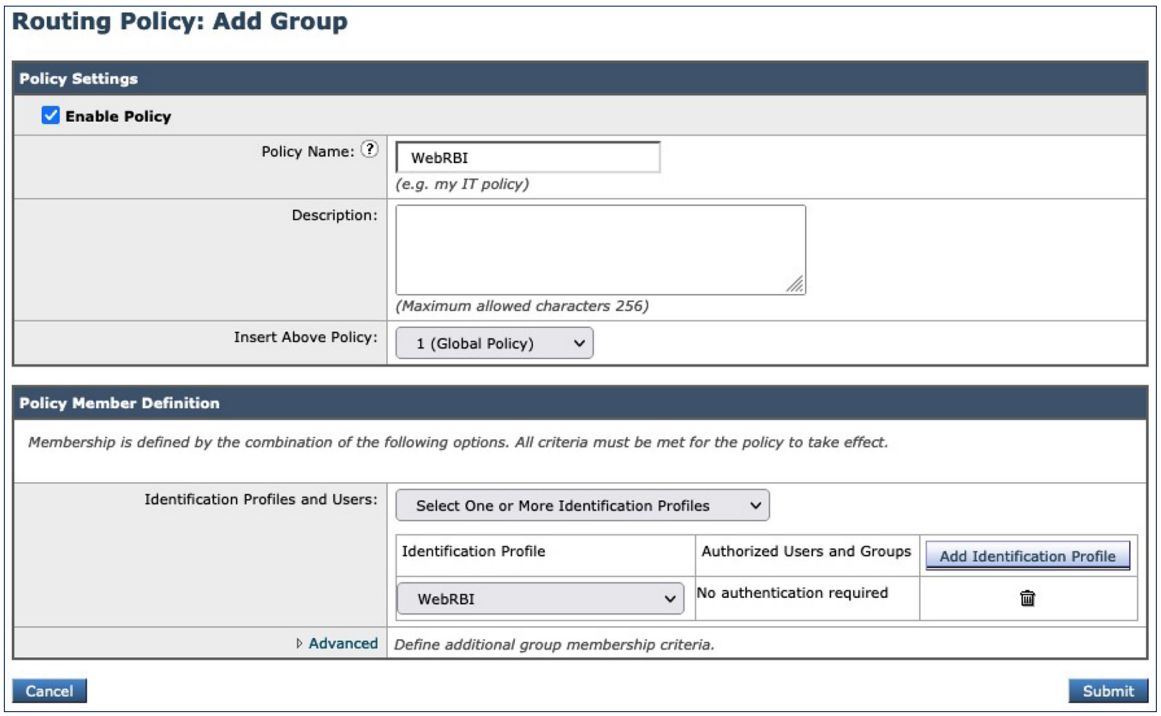
Note: All web traffic will be routed to RBI Security after being inspected by the WSA engine by defining the traffic with HTTP/HTTPS protocol.



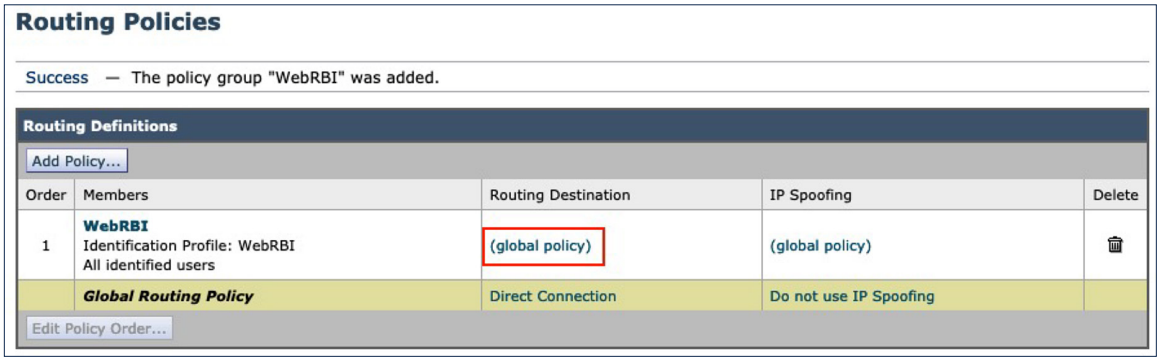
Click the **Submit** button to save the configuration.

Step 6 - Navigate to **Web Security Manager > Routing Policies**, and click on the **Add Policy** button:

Step 7 - Configure the routing policy name and choose an identification profile that was created earlier in step 5. Click the **Submit** button to save the configuration



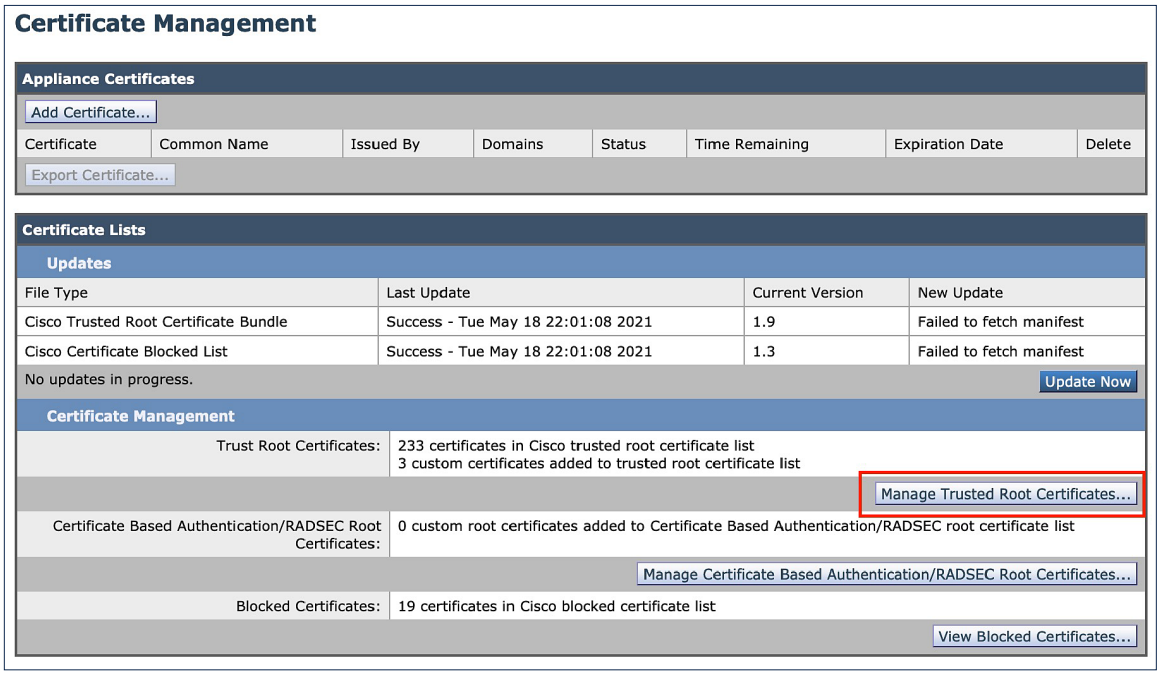
Step 8 - Configure the routing destination with RBI Security as the upstream proxy:



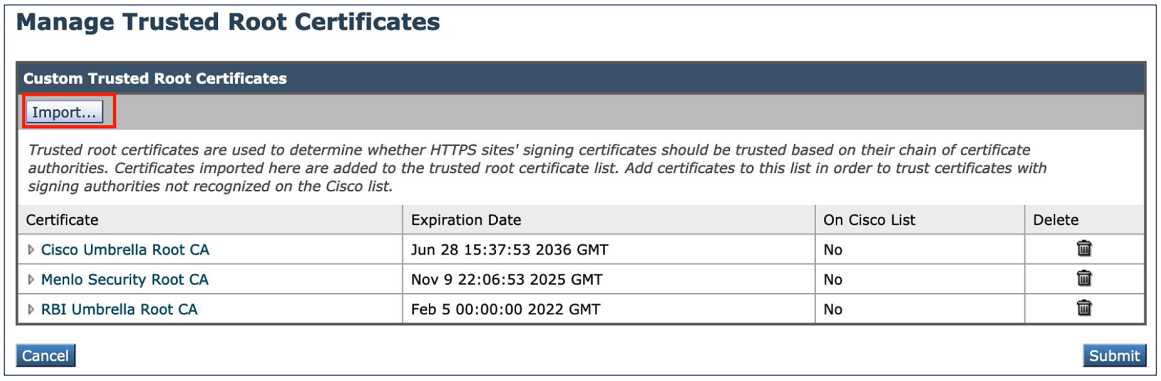
Click the **Submit** button to save the configuration.

Step 9 - For SSL inspection, upload the RBI Security CA certificate to WSA.

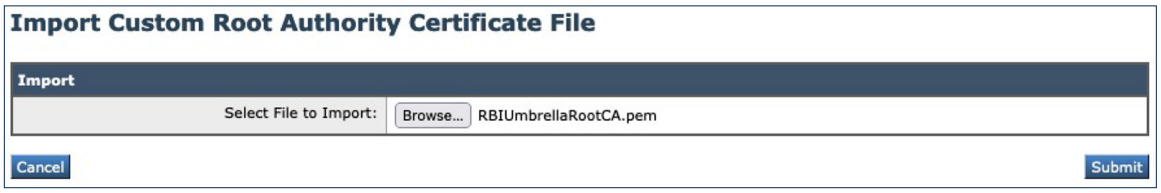
Navigate to **Network > Certificate Management**, and click on the **Manage Trusted Root Certificates** button:



Step 10 - Click the **Import** button under the Custom Trusted Root Certificates section:



Step 11 - Browse to the folder where the RBI Security CA certificate was downloaded earlier.



Click the **Submit** button to upload the certificate.

Click the **Submit** button again to save the configuration.

Step 12 - Click the **Commit Changes** button once the configuration has been completed.

Use cases for selective proxy configuration

The following section walks through a few common use cases adopted by organizations.

Full-coverage browser isolation

The above configuration will allow all web traffic that WSA has inspected to be upstream proxy toward RBI Security. I will walk through the testing step by step and show what is expected to be seen from your web browser to ensure that web traffic has been browser isolated within the RBI Security platform.

Step 1 - Because most web traffic today is HTTPS, ensure that you upload both the WSA and RBI Security HTTPS inspection certificates to your browser before testing.

Step 2 - Explicitly point the user's test machine browser to your WSA.

Step 3 - Browse to a website. In my example, I used https://ipchicken.com/

Step 4 - Ensure that the IP address listed is not your WSA IP address but the RBI Security IP address instead.

Step 5 - Right-click on the website and choose **View Page Source**. The website source will not show the original content page source but the redirection to RBI Security:

For reference, the original website page source looks as follows:

Selectively redirect business-critical web traffic to RBI Security

Most organizations would selectively choose the web traffic to route to the RBI Security platform to ensure that the most critical functions within the organization are protected.

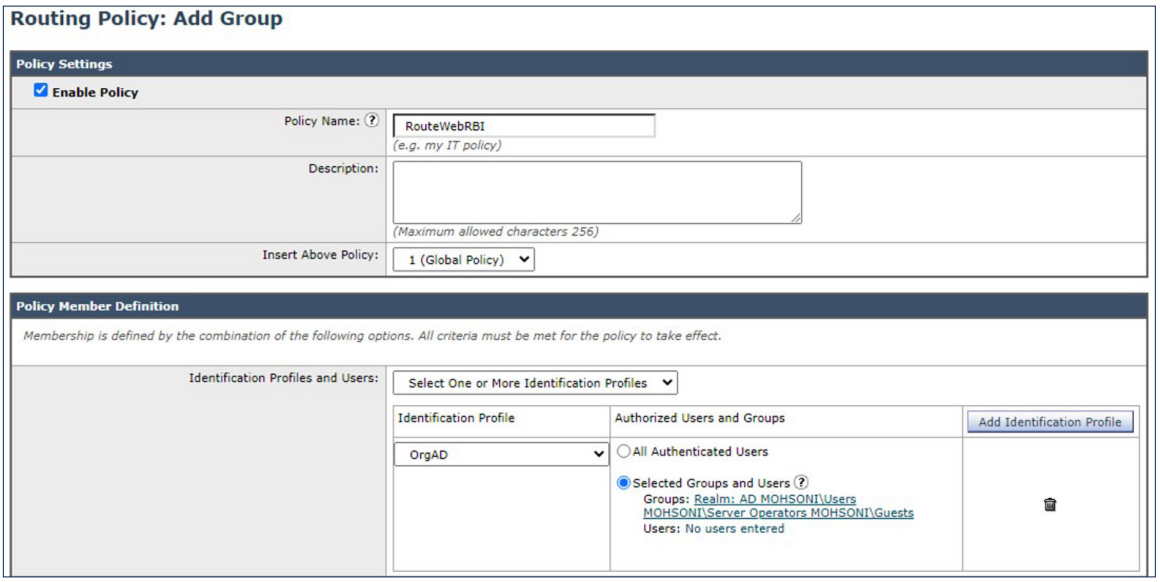
In this use case, two critical groups (engineering and HR/legal) within the organization will have their web traffic selectively routed from the WSA toward RBI Security.

The configuration only needs to be completed on the WSA based on previous configuration steps. We will modify the RBI Security Routing policy to identify those groups (based on AD or LDAP groups).

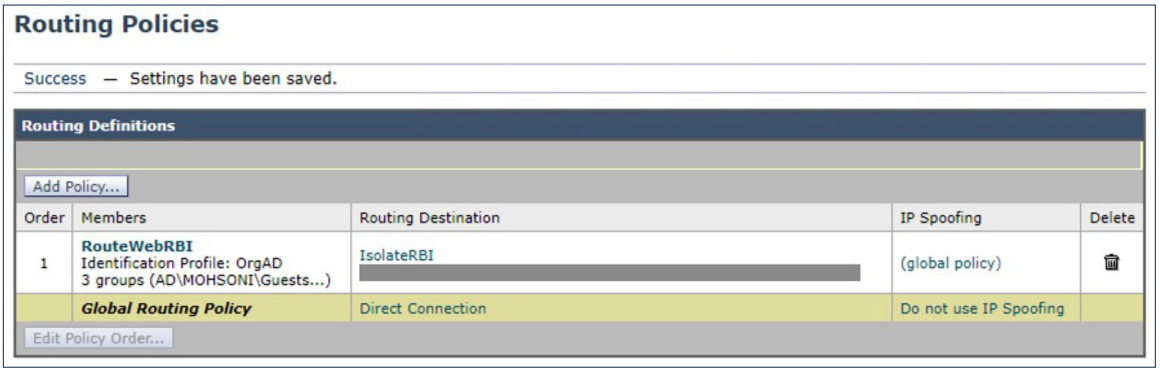
Note: AD configuration is not covered in this guide.

Step 1 - Navigate to **Web Security Manager > Routing Policies**, and edit the existing **RBI Security Routing** under the Members column.

Step 2 - Change the identification profile from **RBI Security Traffic** to the organization AD identification profile and choose the groups:

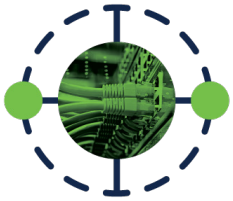


Click the **Submit** button to save the configuration.



Step 3 - Click the **Commit Changes** button upon completing configuration.

Only web traffic from the groups will be an upstream proxy to RBI Security with the above configuration. All other web traffic routes directly to the internet.



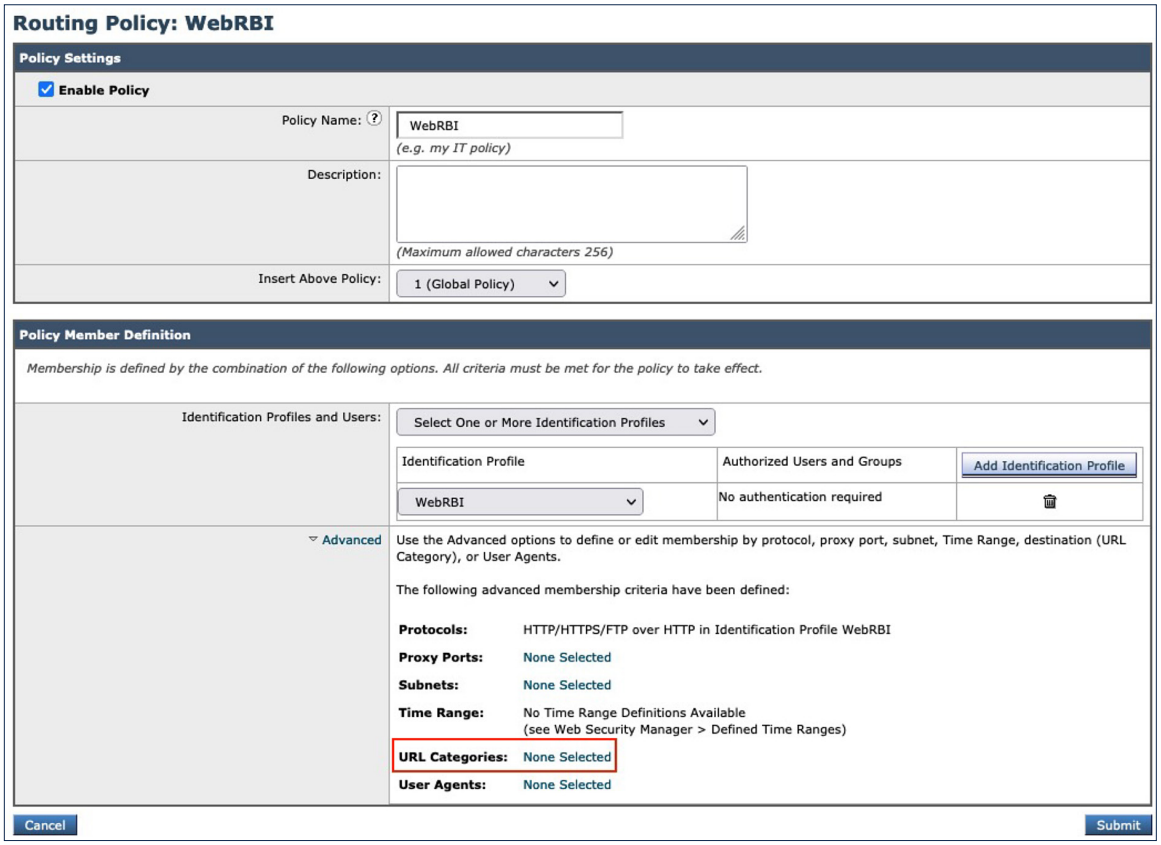
Selectively redirect uncategorized web traffic to RBI Security

Another common scenario that organizations employ is to upstream proxy only uncategorized URLs to RBI Security. We will modify the RBI Security Routing policy to identify only uncategorized URLs as an upstream proxy to RBI.

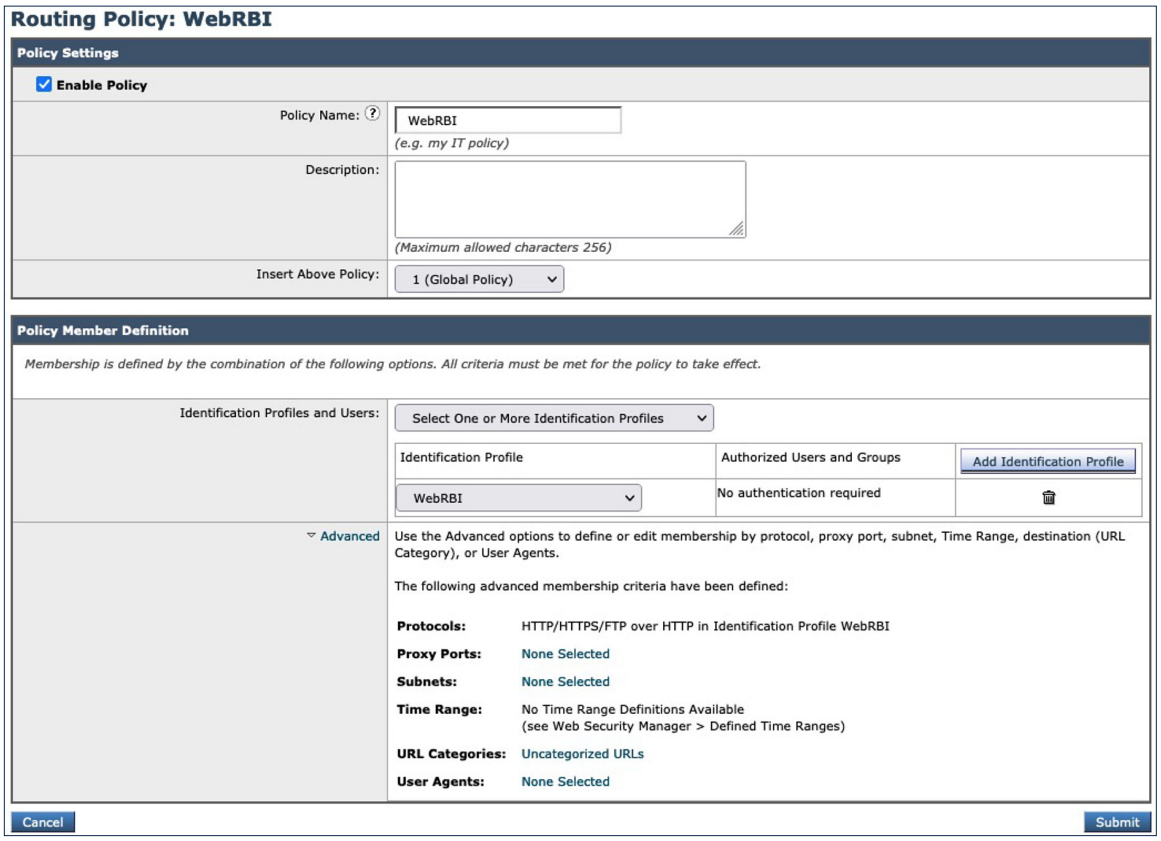
Step 1 – Navigate to **Web Security Manager > Routing Policies**, and edit the existing RBI Security Routing under the Members column.

Step 2 – Update the identification profile back to **RBI Security Traffic** if it hasn't already been configured.

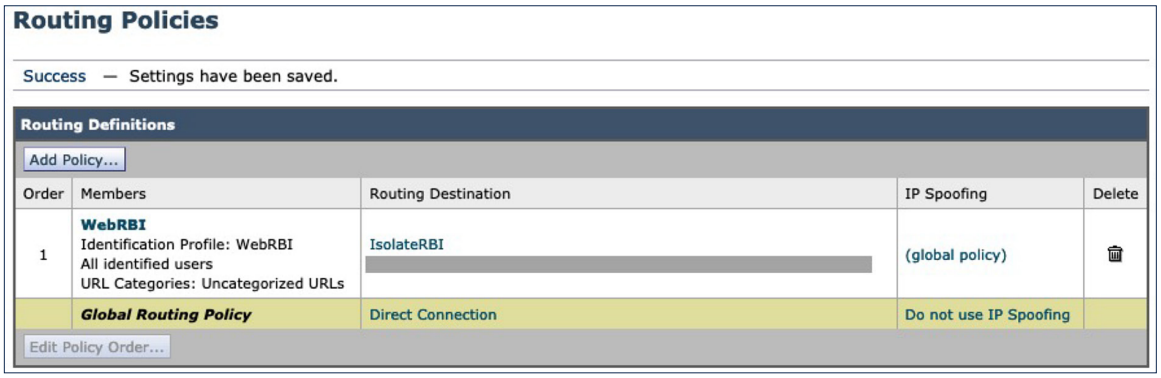
Step 3 – Under the Advanced section, click **URL Categories: None Selected**:



Step 4 – Select **Uncategorized URLs** toward the bottom of the page, and click on the **Done** button:



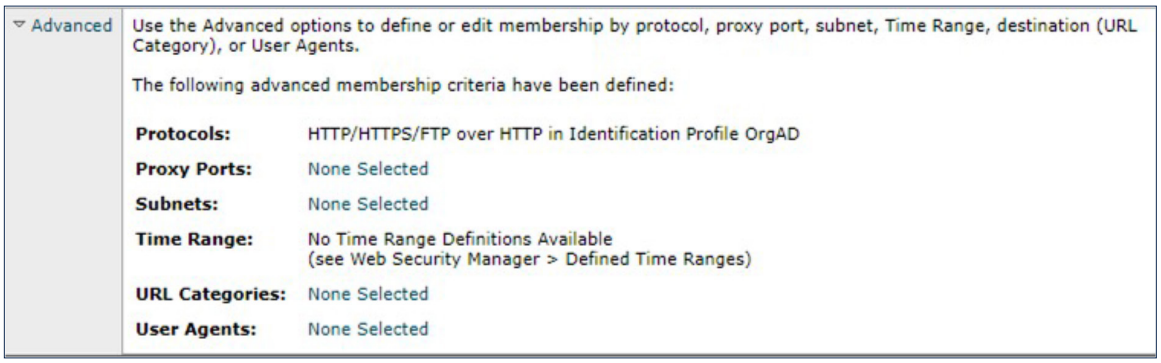
Click the **Submit** button to save the configuration.



Step 5 - Click the **Commit Changes** button once the configuration has been completed.

With the above configuration, all uncategorized web traffic will be upstream proxied to RBI Security for browser isolation. All other web traffic routes directly to the internet.

In summary, the use cases above depict an organization's ability to selectively choose web traffic to be an upstream proxy to RBI Security according to the company's individual needs. Any available fields within the routing policy's Advanced section can be used to route traffic for browser isolation selectively:



Conclusion

In conclusion, why is it important to integrate WSA with RBI Security?

Here are the integration benefits:

- WSA provides the full proxy capabilities, and browser isolation executes web content within an isolated platform instead of in the user's environment.
- WSA provides flexible traffic selection to upstream proxy all web traffic or a subset to allow an admin to route only interesting traffic to RBI Security.
- RBI Security also provides further policy flexibility by allowing specific web categories to be allowed, isolated, isolated with read-only access, or blocked.
- The integration enhances security to protect an organization's environment.

For example, it is impossible to categorize the entire internet; however, blocking uncategorized web traffic is not a solution. For maximum security, routing all uncategorized web traffic from WSA to RBI Security for browser isolation ensures no active content is executed within a user's environment, reducing the risk of infection by attacks.

Package information

Isolate Partial	Isolate Any
• Apply to uncategorized websites • Apply based on user groups (max up to 5 groups) • Choose up to 5 other categories	• Isolate any chosen destination (including content categories, uncategorized URLs, users/groups)

Next steps

For detailed information on Cisco Web Security Appliance, go to www.cisco.com/go/wsa.

A Cisco sales representative, consulting system engineer, or channel partner can help to evaluate how Cisco Web Security Appliance will enhance your security.