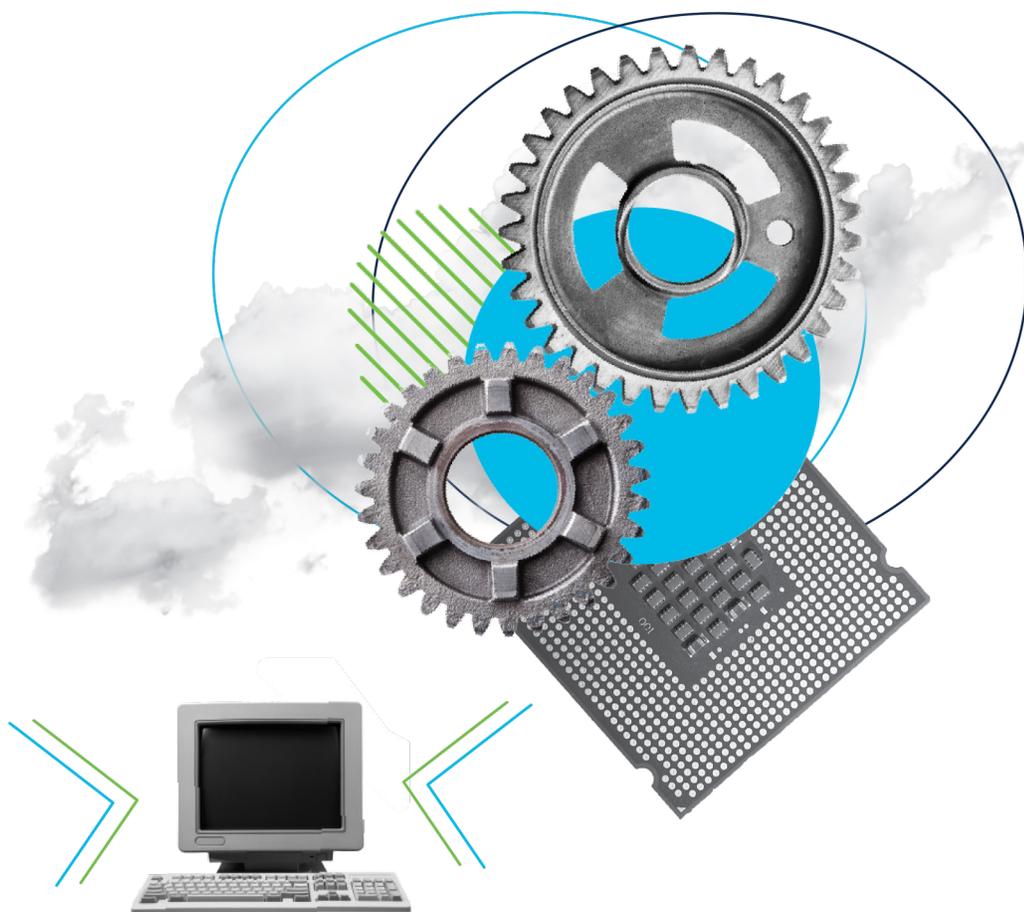


Isolate with Secure Web Appliance



Contents

Overview	3
Introduction to browser isolation technology	3
Product requirements	4
Configuration	4
Use cases for selective proxy configuration	8
Full-coverage browser isolation	8
Selectively redirect business-critical web traffic to RBI Security	9
Selectively redirect uncategorized web traffic to RBI Security	11
Conclusion	13
Package information	13
Next steps	13



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

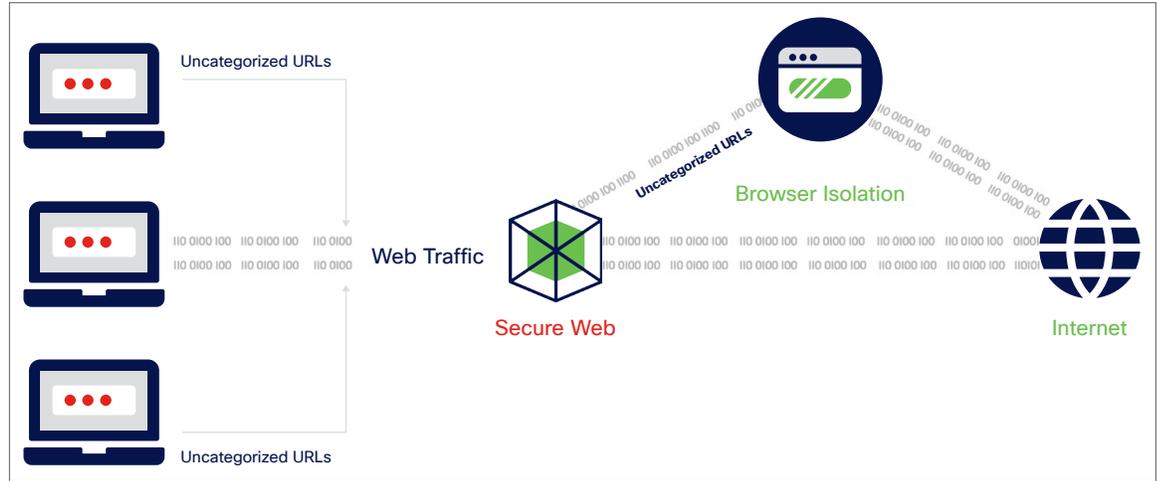
Browser isolation technology provides an added layer of security that isolates any browser-based web traffic to ensure that no web activity is executed locally within a user’s browser—hence eliminating any malware, attack, or infection from being executed within a user’s local network and infrastructure.

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



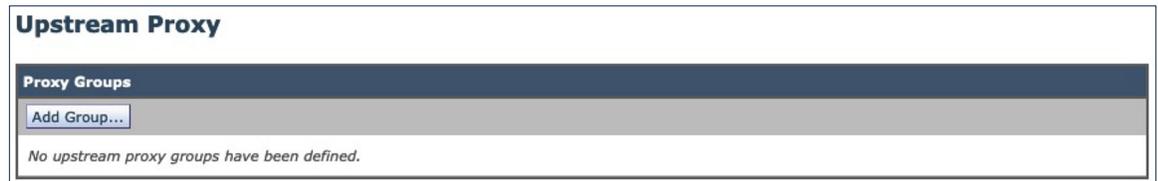
Product requirements

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

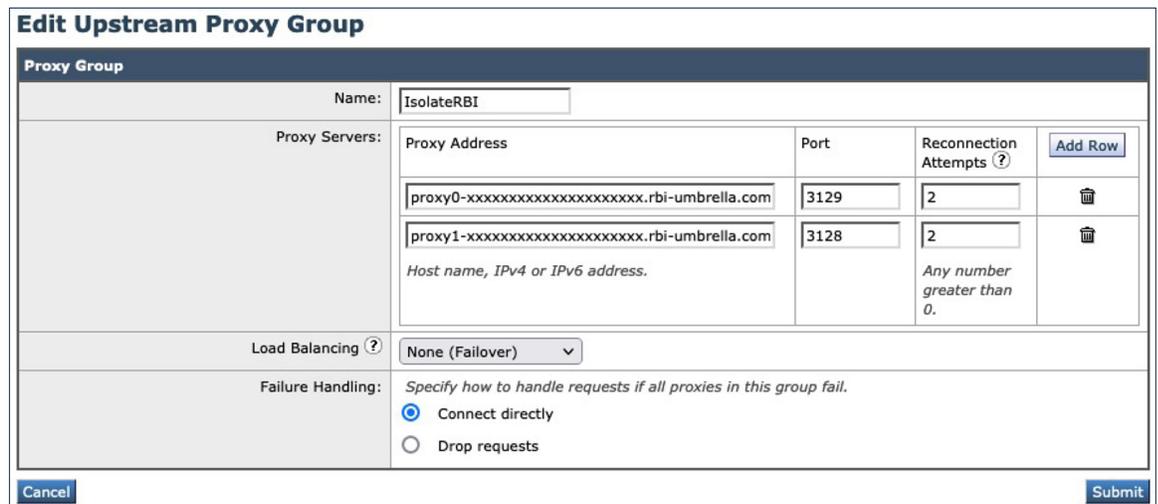
Configuration

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:

Identification Profiles				
Client / User Identification Profiles				
Add Identification Profile...				
Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	
Edit Order...				

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.

Identification Profiles: Add Profile	
Client / User Identification Profile Settings	
<input checked="" type="checkbox"/> Enable Identification Profile	
Name: ?	WebRBI <small>(e.g. my IT Profile)</small>
Description:	<input type="text"/> <small>(Maximum allowed characters 256)</small>
Insert Above:	1 (Global Profile) v
User Identification Method	
Identification and Authentication: ?	Exempt from authentication / identification v <small>This option may not be valid if any preceding Identification Profile requires authentication on all subnets.</small>
Membership Definition	
<small>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</small>	
Define Members by Subnet:	<input type="text"/> <small>(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)</small>
Define Members by Protocol:	<input checked="" type="checkbox"/> HTTP/HTTPS <input type="checkbox"/> Native FTP
Advanced	<small>Define additional group membership criteria.</small>
Cancel	Submit

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



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

Routing Policies

Routing Definitions

Add Policy...

Order	Members	Routing Destination	IP Spoofing	Delete
	Global Routing Policy	Direct Connection	Do not use IP Spoofing	

Edit Policy Order...

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

Routing Policy: Add Group

Policy Settings

Enable Policy

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

Description: (Maximum allowed characters 256)

Insert Above Policy: ▼

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	<input type="button" value="Add Identification Profile"/>
<input type="text" value="WebRBI"/> ▼	No authentication required	<input type="button" value="🗑"/>

Define additional group membership criteria.

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

Routing Policies

Success — The policy group "WebRBI" was added.

Routing Definitions

Add Policy...

Order	Members	Routing Destination	IP Spoofing	Delete
1	WebRBI Identification Profile: WebRBI All identified users	(global policy)	(global policy)	<input type="button" value="🗑"/>
	Global Routing Policy	Direct Connection	Do not use IP Spoofing	

Edit Policy Order...



Routing Policies: Add Upstream Proxy Group

Routing Destination Settings

Upstream Proxy Group: IsolateRBI

Cancel
Submit

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:

Certificate Management

Appliance Certificates

Add Certificate...

Certificate	Common Name	Issued By	Domains	Status	Time Remaining	Expiration Date	Delete
Export Certificate...							

Certificate Lists

Updates

File Type	Last Update	Current Version	New Update
Cisco Trusted Root Certificate Bundle	Success - Tue May 18 22:01:08 2021	1.9	Failed to fetch manifest
Cisco Certificate Blocked List	Success - Tue May 18 22:01:08 2021	1.3	Failed to fetch manifest
No updates in progress. Update Now			

Certificate Management

Trust Root Certificates:	233 certificates in Cisco trusted root certificate list 3 custom certificates added to trusted root certificate list	Manage Trusted Root Certificates...
Certificate Based Authentication/RADSEC Root Certificates:	0 custom root certificates added to Certificate Based Authentication/RADSEC root certificate list	Manage Certificate Based Authentication/RADSEC Root Certificates...
Blocked Certificates:	19 certificates in Cisco blocked certificate list	View Blocked Certificates...

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

Manage Trusted Root Certificates

Custom Trusted Root Certificates

Import...

Trusted root certificates are used to determine whether HTTPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

Certificate	Expiration Date	On Cisco List	Delete
▶ Cisco Umbrella Root CA	Jun 28 15:37:53 2036 GMT	No	🗑️
▶ Menlo Security Root CA	Nov 9 22:06:53 2025 GMT	No	🗑️
▶ RBI Umbrella Root CA	Feb 5 00:00:00 2022 GMT	No	🗑️

Cancel
Submit



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

Import Custom Root Authority Certificate File

Import

Select File to Import: RBIUmbrellaRootCA.pem

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

Manage Trusted Root Certificates

Custom Trusted Root Certificates

Trusted root certificates are used to determine whether HTTPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

Certificate	Expiration Date	On Cisco List	Delete
▶ RBI Umbrella Root CA	Feb 5 00:00:00 2022 GMT	No	🗑️

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

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

Uncommitted Changes

Attention — ⚠️ In order to process these changes, the proxy process will restart after Commit. This will cause a brief interruption in service.

Commit Changes

You have uncommitted changes. These changes will not go into effect until you commit them.

Comment (optional):

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.



Routing Policy: Add Group

Policy Settings

Enable Policy

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

Description: (Maximum allowed characters 256)

Insert Above Policy:

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="OrgAD"/>	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users (?) <small>Groups: Realm: AD\MOHSONI\Users MOHSONI\Server_Operators MOHSONI\Guests Users: No users entered</small>	

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

Routing Policies

Success — Settings have been saved.

Routing Definitions

Add Policy...

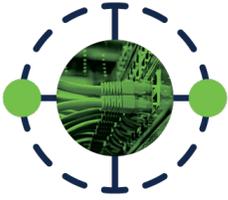
Order	Members	Routing Destination	IP Spoofing	Delete
1	RouteWebRBI Identification Profile: OrgAD 3 groups (AD\MOHSONI\Guests...)	IsolateRBI	(global policy)	
	Global Routing Policy	Direct Connection	Do not use IP Spoofing	

Edit Policy Order...

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**:

Routing Policy: WebRBI

Policy Settings

Enable Policy

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

Description:
(Maximum allowed characters 256)

Insert Above Policy:

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="WebRBI"/>	No authentication required	<input type="button" value="Add Identification Profile"/>

Advanced Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: HTTP/HTTPS/FTP over HTTP in Identification Profile WebRBI

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)

URL Categories: None Selected

User Agents: None Selected

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

Uncategorized URLs

Uncategorized URLs	<input checked="" type="checkbox"/>
--------------------	-------------------------------------



Routing Policy: WebRBI

Policy Settings

Enable Policy

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

Description: (Maximum allowed characters 256)

Insert Above Policy:

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="WebRBI"/>	No authentication required	

Advanced Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

- Protocols:** HTTP/HTTPS/FTP over HTTP in Identification Profile WebRBI
- Proxy Ports:** None Selected
- Subnets:** None Selected
- Time Range:** No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
- URL Categories:** Uncategorized URLs
- User Agents:** None Selected

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

Routing Policies

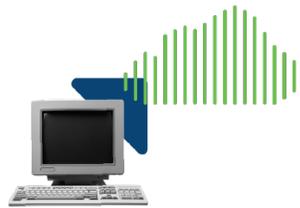
Success — Settings have been saved.

Routing Definitions				
Order	Members	Routing Destination	IP Spoofing	Delete
1	WebRBI Identification Profile: WebRBI All identified users URL Categories: Uncategorized URLs	IsolateRBI	(global policy)	
	Global Routing Policy	Direct Connection	Do not use IP Spoofing	

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:



▼ Advanced	<p>Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.</p> <p>The following advanced membership criteria have been defined:</p> <p>Protocols: HTTP/HTTPS/FTP over HTTP in Identification Profile OrgAD</p> <p>Proxy Ports: None Selected</p> <p>Subnets: None Selected</p> <p>Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)</p> <p>URL Categories: None Selected</p> <p>User Agents: None Selected</p>
------------	---

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
<ul style="list-style-type: none"> • Apply to uncategorized websites • Apply based on user groups (max up to 5 groups) • Choose up to 5 other categories 	<ul style="list-style-type: none"> • 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.