

# Cisco WSA Integration with Menlo Security: Browser Isolation Technology

## Overview

With the current exponentially ever-changing cyber threat landscape, it is becoming increasingly difficult to ensure zero attack, zero malware, and zero infection affecting your organization. Providing a complete security means lowering the number of attacks, malwares, and infections to as close to zero as possible. This can be achieved by integrating the market's best-in-class products.

User expectation when accessing information has also changed considerably where speed, efficiency, and efficacy are the major requirements. Web browsing is now expected through any means, whether the user is connected through LAN, wireless network, satellite, or mobile network connection. It is expected to be available at the tip of your finger and browsing speed should be reasonably fast. Accessibility and faster speed mean more inspections are required on web traffic. Therefore, integration of multiple web security technologies will ensure efficiency in inspecting the web traffic, blocking the attacks and malwares, and stopping infections from propagating through your network.

## About this document

This document describes how to configure Cisco® Web Security Appliance (WSA) to selectively redirect web traffic to Menlo Security Isolation Platform (MSIP) to enhance security by isolating web browsing and document retrieval within the isolation platform.

This document covers:

- Introduction to browser isolation technology
- Cisco product/software and third-party product requirements
- Menlo Security configuration
- Upstream proxy configuration on WSA
- Use cases for selective proxy configuration
- Conclusion
- Next steps

## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

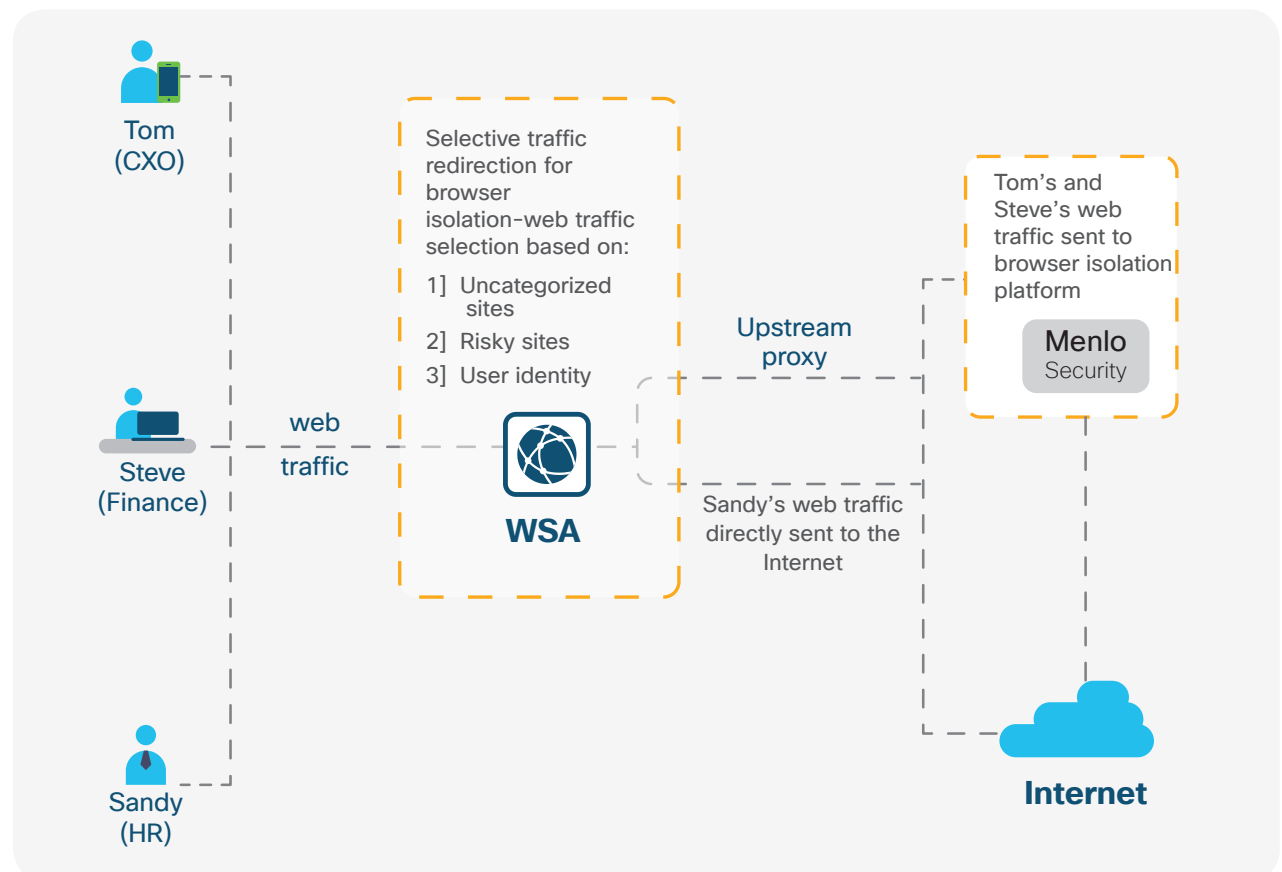
### Next steps

## Introduction to browser isolation technology

Browser isolation technology is next-generation web security that isolates any browser-based web traffic through its browser isolation platform. This ensures that no web activity is being executed locally within a user's browser, hence eliminating any malware, attack, or infection being executed within a user's local network and infrastructure.

In this document, we will be integrating WSA with MSIP, which ensures any malwares or attacks that can be stopped locally by WSA will be detected, hence increasing speed and efficiency, with additional security provided by Menlo Security to enhance efficacy.

### End-to-end web traffic flow diagram



## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

## Cisco product/software and third-party product requirements

- WSA (all hardware and virtual platforms are supported)
- Menlo Security (cloud)

## Menlo Security configuration

**Step 1** - Log in to Menlo Security portal using admin credential: <https://admin.menlosecurity.com/>.

**Step 2** - Navigate to **Settings > Authentication > Corporate Gateway IPs**. Add the WSA gateway IP address(es):

**Step 3** - Click **Save Changes** to submit the IP address(es).

This configuration will authenticate web traffic from your corporate WSA(s) to perform the browser isolation on the Menlo Security cloud.

**Step 4** - Navigate to **Settings > Proxy Auto Config**. On the **Standard** PAC line, click **Actions > Preview**.

## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

**Step 5** - Browse to the end of the PAC file and take note of the two Menlo Security proxy addresses as well as the port numbers within the following sections:

```
if ( url.substring(0, 6) == 'https:' )
{
  return 'PROXY proxy0-XXXXXXXXXX.menlosecurity.com:3129; PROXY proxy1-XXXXXXXXXX.menlosecurity.com:3129; DIRECT';
}

if ( url.substring(0, 5) == 'http:' )
{
  return 'PROXY proxy0-XXXXXXXXXX.menlosecurity.com:3129; PROXY proxy1-XXXXXXXXXX.menlosecurity.com:3129; DIRECT';
}
```

**Note:** If only HTTP web traffic is sent from WSA to Menlo Security, Menlo Security would be accepting traffic on port 3128. If both HTTP and HTTPS web traffic are sent, Menlo Security would be accepting traffic on port 3129 as noted above.

**Step 6** - Lastly, to perform Secure Sockets Layer (SSL) inspection, obtain a copy of the Menlo Security CA certificate from <https://support.menlosecurity.com/instructions/cert/index.html>.

The certificate will later need to be uploaded to WSA and the user browser.

## Upstream proxy configuration on WSA

**Step 1** - Log in to the WSA UI using admin credential: [https://wsa\\_hostname:8443](https://wsa_hostname:8443).

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



**Step 3** - Configure the upstream proxy name and the two proxy server FQDNs (**proxy0-XXXXXXXXXX.menlosecurity.com** and **proxy1-XXXXXXXXXX.menlosecurity.com**) that were noted from the Menlo Security portal (PAC configuration). Click the **Submit** button to save the configuration.

# Contents

## Overview

## About this document

## Introduction to browser isolation technology

## Cisco product/software and third-party product requirements

## Menlo Security configuration

## Upstream proxy configuration on WSA

## Use cases for selective proxy configuration

## Conclusion

## Next steps

**Note:** Replace <customerhash> with the actual hash listed in your Menlo Security portal PAC configuration.

### Add Upstream Proxy Group

Proxy Group			
Name:	<input type="text" value="Menlo Security"/>		
Proxy Servers:	Proxy Address	Port	Reconnection Attempts <sup>?</sup>
	<input type="text" value="proxy0-&lt;customerhash&gt;.menlosecurity.com"/>	<input type="text" value="3129"/>	<input type="text" value="2"/>
	<input type="text" value="proxy1-&lt;customerhash&gt;.menlosecurity.com"/>	<input type="text" value="3129"/>	<input type="text" value="2"/>
	<i>Host name, IPv4 or IPv6 address.</i>		<i>Any number greater than 0.</i>
			<input type="button" value="Add Row"/>
Load Balancing <sup>?</sup>	<input type="button" value="None (Failover)"/> <span style="font-size: small;">⌵</span>		
Failure Handling:	<i>Specify how to handle requests if all proxies in this group fail.</i>		
	<input checked="" type="radio"/> Connect directly <input type="radio"/> Drop requests		
<input type="button" value="Cancel"/>		<input type="button" value="Submit"/>	

**Note:** The proxy address can also be replaced with the IP address.

**Step 4 -** Create the identification profile to determine the web traffic to be selectively proxied from WSA to Menlo Security.

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

### Identification Profiles

Client / User Identification Profiles				
<input type="button" value="Add Identification Profile..."/>				
Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete

**Step 5 -** Configure a placeholder for web traffic identification to be upstream proxy to Menlo Security. In the next section, we will discuss different use cases in which configuration can easily be modified on the identification profile.

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

## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

### Identification Profiles: Add Profile

Client / User Identification Profile Settings	
<input checked="" type="checkbox"/> <b>Enable Identification Profile</b>	
Name: ?	<input type="text" value="Menlo Security Traffic"/> <small>(e.g. my IT Profile)</small>
Description:	<input type="text"/>
Insert Above:	4 (Global Profile) <input type="button" value="v"/>

User Identification Method	
Identification and Authentication: ?	<small>For additional options, define an authentication realm (see Network &gt; Authentication) or enable ISE (see Network &gt; Identity Services Engine).</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	<p>Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents.</p> <p>The following advanced membership criteria have been defined:</p> <p><b>Proxy Ports:</b> None Selected <b>URL Categories:</b> None Selected <b>User Agents:</b> None Selected</p> <p><small>The advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories, are not applicable for transparent HTTPS (unless decrypted). When advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.</small></p>

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

## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

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

Order	Members	Routing Destination	Delete
-------	---------	---------------------	--------

**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.

Identification Profile	Authorized Users and Groups	
Menlo Security Traffic	No authentication required	

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

Upstream Proxy Group:	Menlo Security
-----------------------	----------------

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

## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

**Step 9** - For SSL inspection, upload the Menlo 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 - Wed Aug 29 10:37:06 2018	1.4	Failed to fetch manifest
Cisco Certificate Blacklist	Success - Wed Aug 29 10:37:06 2018	1.3	Failed to fetch manifest

No updates in progress. [Update Now](#)

**Certificate Management**

Trust Root Certificates: 365 certificates in Cisco trusted root certificate list  
1 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
-------------	-----------------	---------------	--------



## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

**Step 11** - Browse to the folder where the Menlo Security CA certificate was downloaded earlier from <https://support.menlosecurity.com/instructions/cert/index.html>.

**Import Custom Root Authority Certificate File**

Import

Select File to Import:  MenloSecurityRootCA.crt

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
↳ Menlo Security Root CA	Feb 1 00:00:00 2019 GMT	No	<input type="button" value="Delete"/>

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

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

**Uncommitted Changes**

**Commit Changes**

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

Comment (optional):





## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

## Selectively redirect business critical web traffic to Menlo Security

Most organizations would selectively choose what web traffic is to be routed to the Menlo Security platform. This ensures that the most critical functions within the organization are protected further.

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

Configuration will only need to be completed on WSA based on previous configuration steps. We will modify the **Menlo Security Routing** policy to identify those groups (based on AD or LDAP groups). Note: AD configuration will not be covered in this guide.

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

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

**Routing Policy: Menlo Security Routing**

**Policy Settings**

Enable Policy

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

Description:

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="button" value="CompanyA AD"/>	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users <small>?</small> Groups: Realm: <b>WSABU</b> CISCOWSABU\Eng CISCOWSABU\HR Users: No users entered	<input type="button" value=""/>

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

## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration


### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

Success — Settings have been saved.

Routing Definitions			
Add Policy...			
Order	Members	Routing Destination	Delete
1	<b>Menlo Security Routing</b> Identification Profile: CompanyA AD 2 groups (WSABU\CISCOWSABU\Eng...)	Menlo Security	
	<b>Global Routing Policy</b>	Direct Connection	

Edit Policy Order...

**Step 3** - Click the **Commit Changes** button once configuration has been completed.

With the above configuration, only web traffic from the engineering and HR groups will be upstream proxy to Menlo Security. All other web traffic will be routed directly to the Internet.

### Selectively redirect uncategorized web traffic to Menlo Security

Another common scenario that organizations employ is to upstream proxy only uncategorized URLs to be routed to Menlo Security. We will modify the **Menlo Security Routing** policy to identify only uncategorized URLs to be upstream proxy to Menlo.

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

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

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

## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

### Routing Policy: Menlo Security Routing

**Policy Settings**

Enable Policy

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

Description:

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="text" value="Menlo Security Traffic"/>	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 Menlo Security Traffic
- Proxy Ports: None Selected
- Subnets: None Selected
- Time Range: None Selected
- URL Categories: None Selected**
- User Agents: None Selected

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

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

## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

### Routing Policy: Menlo Security Routing

**Policy Settings**

- Enable Policy
- Policy Name:   
(e.g. my IT policy)
- Description:
- 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:	Authorized Users and Groups	
<input type="text" value="Select One or More Identification Profiles"/>	<input type="text" value="No authentication required"/>	<input type="button" value="Add Identification Profile"/>
<input type="text" value="Menlo Security Traffic"/>		<input type="button" value=""/>

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 Menlo Security Traffic
- Proxy Ports:** None Selected
- Subnets:** None Selected
- Time Range:** None Selected
- URL Categories:** Uncategorized URLs
- User Agents:** None Selected

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

# Contents

## Overview

## About this document

## Introduction to browser isolation technology

## Cisco product/software and third-party product requirements

## Menlo Security configuration

## Upstream proxy configuration on WSA


## Use cases for selective proxy configuration

## Conclusion

## Next steps

**Routing Policies**

Success — Settings have been saved.

Routing Definitions			
Add Policy...			
Order	Members	Routing Destination	Delete
1	<b>Menlo Security Routing</b> Identification Profile: Menlo Security Traffic All identified users URL Categories: Uncategorized URLs	Menlo Security	
	<b>Global Routing Policy</b>	Direct Connection	

Edit Policy Order...

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

With the above configuration, all uncategorized web traffic will be upstream proxy to Menlo Security so it gets browser isolated. All other web traffic will be routed directly to the Internet.

In summary, based on the above use cases, the organization can selectively choose web traffic to be upstream proxy to Menlo Security according to the company's individual needs. Any available fields within the **Advanced** section of the routing policy can be used to selectively route traffic to be browser isolated:

▼ 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:  <b>Protocols:</b> HTTP/HTTPS/FTP over HTTP in Identification Profile Menlo Security Traffic <b>Proxy Ports:</b> None Selected <b>Subnets:</b> None Selected <b>Time Range:</b> None Selected <b>URL Categories:</b> None Selected <b>User Agents:</b> None Selected
------------	---



## Contents

### Overview

### About this document

### Introduction to browser isolation technology

### Cisco product/software and third-party product requirements

### Menlo Security configuration

### Upstream proxy configuration on WSA

### Use cases for selective proxy configuration

### Conclusion

### Next steps

## Conclusion

In conclusion, why do we think it is important to integrate WSA with Menlo Security?

Here is a list of the benefits of integration:

- WSA provides the full proxy capabilities, and with Menlo Security browser isolation, it executes the web content within an isolated platform instead of the user's environment.
- WSA provides flexible traffic selection to upstream proxy all web traffic or a subset, which will allow an admin to route only interested traffic to Menlo Security.
- Menlo Security also provides further policy flexibility by allowing specific web categories to be allowed, isolated, isolated with read-only access, or blocked.
- The integration will enhance security to further protect the organization's environment. For example, it is impossible to categorize the entire Internet; however, blocking uncategorized web traffic is also not a solution. For maximum security, routing all uncategorized web traffic from WSA to Menlo Security to be browser isolated will ensure no active content is executed within a user's environment, hence reducing risk of infection or attack.

## Next steps

For detailed information on Cisco Web Security Appliance, go to [www.cisco.com/go/wsa](http://www.cisco.com/go/wsa).

Find out more about Menlo Security at [www.menlosecurity.com/](http://www.menlosecurity.com/).

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