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

© 2018 Cisco and/or its affiliates. All rights reserved.
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
Cisco product/software and third-party product requirements

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

Menlo Security configuration


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

![Corporate Gateway IPs](image)

**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**.

![Proxy Automatic Configuration](image)
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:

```javascript
if (url.startsWith('http://')) {
  return 'proxy0-<customerhash>.menlosecurity.com:3128 proxy1-<customerhash>.menlosecurity.com:3129 DIRECT';
}
if (url.startsWith('https://')) {
  return 'proxy0-<customerhash>.menlosecurity.com:3129 proxy1-<customerhash>.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](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-<customerhash>.menlosecurity.com` and `proxy1-<customerhash>.menlosecurity.com`) that were noted from the Menlo Security portal (PAC configuration). Click the **Submit** button to save the configuration.
Note: Replace `<customerhash>` with the actual hash listed in your Menlo Security portal PAC configuration.

### 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:

### 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.
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 Menlo Security as the upstream proxy:

Click the Submit button to save the configuration.
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:

Step 10 - Click the Import button under the Custom Trusted Root Certificates section:
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](image1)

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

![Manage Trusted Root Certificates](image2)

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

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

![Uncommitted Changes](image3)
Use cases for selective proxy configuration

In the following section, we will walk through a few common use cases adopted by organizations.

Full-coverage browser isolation

The above configuration will allow all web traffic that has been inspected by WSA to be upstream proxy towards Menlo 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 Menlo Security platform.

Step 1 - Because most web traffic today is HTTPS, ensure that you have uploaded both the WSA and Menlo Security HTTPS inspection certificate to your browser prior to testing.

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

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

Step 4 - Ensure that the IP address listed is not your WSA IP address but the Menlo 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 Menlo Security:
For reference, the original website page source looks like the following:

On the Menlo Security admin portal, you would see a log indicating that the [https://ipchicken.com](https://ipchicken.com) webpage has been browser isolated.

<table>
<thead>
<tr>
<th>Date</th>
<th>User ID</th>
<th>URL</th>
<th>Categories</th>
<th>Threat Type</th>
<th>Details</th>
<th>User Agent</th>
<th>Request Type</th>
<th>Risk</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/12/2018</td>
<td></td>
<td><a href="https://ipchicken.com/">https://ipchicken.com/</a></td>
<td>Computers &amp; Technology</td>
<td></td>
<td>Firefox 62</td>
<td>Page Request</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12/12/2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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:

Click the Submit button to save the configuration.
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:
Step 4 - Select **Uncategorized URLs** towards 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 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:
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.

Find out more about Menlo Security at 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.