Overview

The current cyber threat landscape has continually increased in an alarming rate. Technology sophistication comes with a hefty price that consumers have to pay. From mobile threats to targeted attacks, organizations are now focusing on tightening security and decreasing the amount of threats that hit both inbound and outbound flows.

Cisco® security has been focusing on an overall architectural approach to combat the current cyber threats. In the past, a single technology or product was offered, as the attacks were very targeted. Today, the same methodology is becoming less effective. Cisco combines the best-in-class products to provide protection across the attack continuum before, during, and after an attack.
Introduction to Cisco’s architectural approach

A single-product approach has become a thing of the past. It would no longer be sufficient or effective in combating threats. During the past few years, an architectural approach was introduced to help ensure end-to-end security. Cisco combines all intelligence collected via different protocols and applications, including Domain Name System (DNS), web (HTTP and HTTPS), FTP, email (Simple Mail Transfer Protocol), and Simple Network Management Protocol, among others, within Talos™ (Cisco threat intelligence).

In this document, we are integrating Cisco Umbrella with WSA to enforce security on multiple layers using DNS and web traffic.

Cisco Umbrella is a cloud security platform that provides the first layer of defense against threats for all applications. DNS is a basic requirement to connect to the Internet, and it provides broad visibility across various endpoints, from servers, workstations and laptops, mobile phones, and managed and unmanaged devices to Internet of Things (IoT) devices.

WSA is a web proxy solution that further enhances security by offering granular web usage controls, including Application Visibility and Control (AVC), and custom headers for compliance. WSA performs deep packet inspection for all web traffic, whether it’s in plain text or it’s encrypted.

The integration between both products will help ensure that organizations are fully protected. This integration will help cover attacks from known good domains hosting malware (WSA) and newly seen domains where Cisco Umbrella has the best coverage. It will also help decrypt all Secure Sockets Layer traffic to help ensure no hidden malware (WSA) and, most importantly, visibility of various attack vectors—not only via DNS or web, but also all via other protocols powered by Talos intelligence.

Cisco products

- WSA, software version 10.5 or later (all hardware and virtual platforms are supported)
- Cisco Umbrella (cloud security)

Integration use cases

We will share some of the most common use cases integrating WSA with Cisco Umbrella.
Mandatory category block

Most organizations have a mandatory global block policy that applies to everyone in the organization. To provide a quick and easy global block policy, we recommend the configuration first be completed on the Cisco Umbrella dashboard, as it is a cloud-delivered solution. It is a quick and easy deployment and provides a first layer of defense. Once that has been accomplished, look into creating detailed filtering of IP addresses and URLs on WSA.

Step 1 – Log in to the Cisco Umbrella dashboard using the admin credential: [https://login.umbrella.com/](https://login.umbrella.com/)

Step 2 – Navigate to Policy > Policy List. Expand Default Policy. Edit Content Setting:
Step 3 – Choose High, Moderate, or Low or create your own Custom category group. Click Set and Return:
Step 4 – Under Content Setting, the chosen content categories will be listed. Click Save to save the settings:

Step 5 – Next, you can configure specific organizational policies on WSA. Some of the use cases include the following:

- AVC configuration for very specific Active Directory (AD) group(s) or user(s)
- Specific URL configuration for specific AD group(s) or user(s)
- Custom category configuration for specific AD group(s) or user(s)
- User agent–based access policy
- Time-based access policy
- Quota-based access policy
Consistent end-user notification page

When integrating multiple products, it is important to have a consistent End-User Notification (EUN) page. With the integration of WSA and Cisco Umbrella, it can be achieved in two ways:

1. Redirect both the EUN from WSA and the EUN from Cisco Umbrella to a custom URL (for example, a EUN or block page hosted on the organization’s web server).

To configure custom URL redirection on WSA, navigate to Security Services > End-User Notification and click the Edit Settings button:

End-user notification
Then navigate to the **End-User Notification Pages** section > **Notification Type** and choose **Redirect to Custom URL** > **Notification Page URL**. Type the URL of the EUN page hosted within your web server:

![End-User Notification Pages](image)

To configure custom URL redirection on Cisco Umbrella, navigate to **Policies > Block Page Appearance** and expand **Default Settings > Redirect users to this URL**. Type the URL of the EUN page hosted within your web server:

![Redirect users to this URL](image)

2. Alternatively, use only the WSA EUN or block page for consistency. To configure the use of a WSA block page when Cisco Umbrella is presenting its block page, configure an access policy on WSA to block the following Cisco Umbrella block pages: [https://support.umbrella.com/hc/en-us/articles/115001357688-What-are-the-Cisco-Umbrella-Block-Page-IP-Addresses](https://support.umbrella.com/hc/en-us/articles/115001357688-What-are-the-Cisco-Umbrella-Block-Page-IP-Addresses).

When a user browses to the Cisco Umbrella block page, the WSA access policy is configured to block those pages. In turn, the user will be presented with the WSA block page.
In WSA, navigate to **Web Security Manager > Custom and External URL Categories** and click the **Add Category** button under **Sites**. Include all IP addresses listed in the Cisco Umbrella block pages article:

### Custom and external URL categories: Add category

![Custom and external URL categories: Add category](image)

Next, configure the block access policy for the above Cisco Umbrella block custom category. Navigate to **Web Security Manager > Access Policies** and click the **Add Policy** button. Under **URL Categories**, choose **Umbrella block category**:
Organizations are looking to maximize security on multiple products. For WSA and Cisco Umbrella integration, we recommend that the following security settings be deployed to achieve the highest level of security.

DNS-based security in Cisco Umbrella will prevent organizations from the following threats: malware, newly seen domains, command and control, phishing attacks, dynamic DNS, potentially harmful domains, DNS tunneling VPN, and cryptomining.

To enable this security setting in Cisco Umbrella, navigate to Policies > Policy List, expand Default Policy, edit Security Setting, and check off all categories to be blocked.
Web-based security on WSA will prevent organizations from further web-based threats, as WSA performs deep packet inspection on all web traffic that passes through WSA. A majority of the threats will be blocked by enabling web reputation filtering in which sites with low scores are blocked. Further threats like adware, malware, spyware, Trojans, viruses, worms, and outbreak heuristics will also be blocked by WSA.
To enable this security setting in WSA, navigate to **Web Security Manager > Access Policies** and edit **Anti-Malware and Reputation** in **Global Policy**:

**Web Reputation Settings**

Web Reputation Filters will automatically block transactions with a low Web Reputation score. For transactions with a higher Web Reputation score, scanning will be performed using the services selected by Adaptive Scanning.

If Web Reputation Filtering is disabled in this policy, transactions will not be automatically blocked based on low Web Reputation Score. Blocking of sites that contain malware or other high-risk content is controlled by the settings below.

- Enable Web Reputation Filtering

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Advanced Malware Protection Settings**

File Reputation Filters will identify transactions containing known malicious or high-risk files. Files that are unknown may be forwarded to the cloud for File Analysis.

- File Reputation

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Cisco DVB Anti-Malware Settings**

- Enable Suspect User Agent Scanning
- Enable Anti-Malware Scanning (Webroot, McAfee, and Sophos)

<table>
<thead>
<tr>
<th>Malware Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Adware</td>
</tr>
<tr>
<td>✓ Browser Helper Object</td>
</tr>
<tr>
<td>✓ Commercial System Monitor</td>
</tr>
<tr>
<td>✓ Dialer</td>
</tr>
<tr>
<td>✓ Generic Spyware</td>
</tr>
<tr>
<td>✓ Hijacker</td>
</tr>
<tr>
<td>✓ Other Malware</td>
</tr>
<tr>
<td>✓ Prishing URL</td>
</tr>
<tr>
<td>✓ PUA</td>
</tr>
<tr>
<td>✓ System Monitor</td>
</tr>
<tr>
<td>✓ Trojan Downloader</td>
</tr>
<tr>
<td>✓ Trojan Horse</td>
</tr>
<tr>
<td>✓ Trojan Phisher</td>
</tr>
<tr>
<td>✓ Virus</td>
</tr>
<tr>
<td>✓ Worm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Encrypted File</td>
</tr>
<tr>
<td>✓ Outbreak Heuristics</td>
</tr>
<tr>
<td>✓ Suspect User Agents</td>
</tr>
<tr>
<td>✓ Unclassable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Reporting

With the increase implementation of the architectural approach, it is becoming essential that organizations have a single pane of reporting from multiple products. With unified reporting, it is easier for organizations to perform threat analysis, forensic analysis, and investigation for troubleshooting purposes. WSA and Cisco Umbrella have an integrated Advanced Web Security Reporting (AWSR) platform. WSA logs can be sent via FTP or Syslog, and Cisco Umbrella logs can be pulled from the Cisco Umbrella Amazon Web Services (AWS) S3 bucket.


Explicit-mode deployment

In explicit-mode deployment, users will point the proxy setting to WSA. This can be done by pointing directly to WSA or via a PAC (Proxy Auto-Config) file.

Here is a sample of a simple PAC file pointing to WSA as its proxy server:

```javascript
function FindProxyForURL(url, host) {
  // if the hostname matches, send direct.
  if (dnsDomains(host, "intranet.domain.com") ||
      shExpMatch(host, "(*.abcdomain.com|abcdomain.com)")
    )
    return "DIRECT";

  // if the protocol or URL matches, send direct.
  if (url.substring(0, 4) == "ftp:" ||
      shExpMatch(url, "http://abcdomain.com/folder/*")
    )
    return "DIRECT";

  // if the requested website is hosted within the internal network, send direct.
  if (isPlainHostName(host) ||
      shExpMatch(host, ".*local") ||
      isINet(dnsResolve(host, "10.0.0.0","255.0.0.0") ||
      isINet(dnsResolve(host, "172.16.0.0","255.240.0.0") ||
      isINet(dnsResolve(host, "192.168.0.0","255.255.0.0") ||
      isINet(dnsResolve(host, "127.0.0.0","255.255.255.0")
    )
    return "DIRECT";

  // DEFAULT RULE: All other traffic, use below proxies, in fail-over order.
  return "PROXY wsa-address:80;";
```
If you would like to present an individual product block page, the Cisco Umbrella block page IP addresses need to be excluded in the PAC file to go direct:

```javascript
function FindProxyForURL(url, host) {
    // if the hostname matches, send direct.
    if (dnsDomain(host, "intranet.domain.com") ||
        shExpMatch(host, "(*.abcdomain.com|abcdomain.com)") )
        return "DIRECT";

    // if the protocol or URL matches, send direct.
    if (url.substring(0, 4) == "ftp:" ||
        shExpMatch(url, "http://abcdomain.com/folder/"))
        return "DIRECT";

    // If the requested website is hosted within the internal network, send direct.
    if (isPlainHost(host) ||
        shExpMatch(host, "*.local") ||
        isINet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
        isINet(dnsResolve(host), "172.16.0.0", "255.240.0.0") ||
        isINet(dnsResolve(host), "192.168.0.0", "255.255.0.0") ||
        isINet(dnsResolve(host), "127.0.0.0", "255.255.255.0") )
        return "DIRECT";

    // Umbrella block pages, send direct.
    if (isINet(dnsResolve(host), "146.112.61.104", "255.255.255.255") ||
        isINet(dnsResolve(host), "146.112.61.105", "255.255.255.255") ||
        isINet(dnsResolve(host), "146.112.61.106", "255.255.255.255") ||
        isINet(dnsResolve(host), "146.112.61.107", "255.255.255.255") ||
        isINet(dnsResolve(host), "146.112.61.108", "255.255.255.255") ||
        isINet(dnsResolve(host), "146.112.61.109", "255.255.255.255") ||
        isINet(dnsResolve(host), "146.112.61.110", "255.255.255.255") )
        return "DIRECT";

    // DEFAULT RULE: All other traffic, use below proxies, in fail-over order.
    return "PROXY wsa-address:80";
}
```
The updated Cisco Umbrella block IP addresses can be found in this article.

**Best-practice tip:** Configure consistent block pages for both WSA and Cisco Umbrella utilizing the WSA EUN or block page. Do not exclude Cisco Umbrella block page IP addresses in the PAC file to go direct. The connection to the Cisco Umbrella block IP address will be forwarded to WSA via the PAC file, and WSA will be configured with access policy to block those IP addresses, as in our use case example above (“Consistent end-user notification page”).

## Transparent-mode deployment

In transparent-mode deployment, no configuration is required on the user side. DNS is configured to point to Cisco Umbrella. Web traffic will be transparently redirected to WSA via an in-path network device with Web Cache Communication Protocol (WCCP).

Here is an example of a WCCP access list to redirect web traffic to WSA:

```plaintext
access-list wccp-traffic extended permit tcp any any eq http
access-list wccp-traffic extended permit tcp any any eq https
```

If you would like to present an individual product block page, the Cisco Umbrella block page IP addresses need to be excluded in the WCCP access list to go direct:

```plaintext
access-list wccp-traffic extended deny ip any host 146.112.61.104
access-list wccp-traffic extended deny ip any host 146.112.61.105
access-list wccp-traffic extended deny ip any host 146.112.61.106
access-list wccp-traffic extended deny ip any host 146.112.61.107
access-list wccp-traffic extended deny ip any host 146.112.61.108
access-list wccp-traffic extended deny ip any host 146.112.61.109
access-list wccp-traffic extended deny ip any host 146.112.61.110
access-list wccp-traffic extended permit tcp any any eq http
access-list wccp-traffic extended permit tcp any any eq https
```

As with explicit-mode deployment, if you wish to configure consistent block pages for both WSA and Cisco Umbrella by utilizing a WSA EUN or block page, do not exclude Cisco Umbrella block page IP addresses in the WCCP access list to go direct.
Conclusion

Why do we think it is important to integrate WSA with Cisco Umbrella?

Here is a list of the benefits:

- Cisco Umbrella provides in-depth DNS security, and WSA provides in-depth web security.
- Ransomware threat vectors include both DNS and web; hence it is extremely important to provide in-depth security for both protocols.
- DNS threat intelligence provides a first layer of defense within your network and couples with WSA, which further protects and helps ensure compliance within your organization.
- The integration helps remove blind spots within your network by inspecting non-domain-based web traffic.