## Contents

- **Introduction** .................................................................................................................................................. 1  
- **Cloud Deployment** ......................................................................................................................................... 1  
- **Additional Redirect Methods** ..................................................................................................................... 1  
- **Prepare** ......................................................................................................................................................... 2  
  - Verify connection to a tower ............................................................................................................................. 2  
  - Create authentication license key .................................................................................................................... 3  
- **Deploy** ............................................................................................................................................................ 5  
  - Configure ASA connector ................................................................................................................................. 5  
    - Redirect web traffic ......................................................................................................................................... 5  
    - Configure ACL whitelisting ............................................................................................................................ 7  
    - Configure user identity ...................................................................................................................................... 11  
- **Test** ............................................................................................................................................................... 14  
  - Verify web redirection to the cloud .................................................................................................................. 14  
- **Appendix** ....................................................................................................................................................... 15
Introduction

Integrating CWS with the ASA maximizes your ASA/ASAv performance by offloading your content scanning to Cisco’s cloud. It also enables you to apply acceptable use policy to the company, groups or individual users routing through the ASA.

This document provides directions to redirect network traffic to CWS through the ASA.

*Note: we refer to our cloud proxies as towers. You will see the terms “proxy” and “tower” used interchangeably throughout the document.

Cloud Deployment

Deployment is divided into the following three sections

Additional Redirect Methods

There are 4 additional redirection methods that have corresponding deployment guides. Deployment guides for each redirection methods can be found here, under Technical Collateral.

<table>
<thead>
<tr>
<th>Redirection Method</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Integrated Services Router (ISR G2 with CWS Connector)</strong></td>
<td>Save bandwidth, money and resources by intelligently redirecting Internet traffic from branch offices directly to the cloud to enforce security and control policies. Apply acceptable use policy to all users regardless of location.</td>
</tr>
<tr>
<td><strong>Web Security Appliance (WSA/WSAv with CWS Connector)</strong></td>
<td>Integrate CWS and WSA to enable identity information to the cloud and extend other on-premises enterprise features to Cloud Web Security customers</td>
</tr>
<tr>
<td><strong>Cisco AnyConnect Secure Mobility Client (AnyConnect)</strong></td>
<td>Authenticate and redirect web traffic securely whenever the end user is off the corporate network. CWS leverages cached user credentials and directory information when they are away from the office or VPN, ensuring that exactly the same web-usage policies are applied.</td>
</tr>
<tr>
<td><strong>Standalone Deployment</strong></td>
<td>Deploy a simple web security solution that does not require any additional hardware. Connect to Cisco’s Cloud Web Security service using existing browser settings and PAC/WPAD files.</td>
</tr>
</tbody>
</table>
Verify connection to a tower

Site-to-tower communication is accomplished over TCP port 8080. HTTP and HTTPS requests are sent to a cloud scanning tower in this method. Therefore, TCP port 8080 outbound is required to be open for all users within the organization. For security reasons, Cisco recommends that port 8080 outbound destinations be limited to the scanning towers provisioned for the customer’s account.

Reference video: [Verify connection to a tower]

**Step 1:** Log on to a client computer inside the customer’s network.

**Step 2:** Click on the Control Panel and go to Programs and Features.

**Step 3:** Click Turn on Windows features on or off.Scroll down the list of available features until you find the Telnet Client. Check the box and click OK. Now that the Telnet Client is installed, we can resume our test.

![Figure 1.1](image)

**Step 4:** Open the command line window and type command ‘telnet [tower IP address] 8080.” A successful connection is noted by a blank screen and blinking cursor.

![Figure 1.2](image)
Create authentication license key

Reference video: **Authentication license key creation and management**

**Step 1:** Log on to the Cisco Cloud Web Security portal at [https://scancenter.scansafe.com/](https://scancenter.scansafe.com/).

**Step 2:** From the **Admin** tab, mouse over **Authentication**, and select the key that you would like to generate. The options are Company Key to have a single key for all users in the company (can be used in various Connectors), AnyConnect, or a mixture of them all.

**Step 3:** Notice that no Company Key currently exists in this account. Click the Create Key button to create the Company Key. If one already exists and you don’t know the whole string (only the last four characters will be seen), then you will have to revoke it before you can create a new one, but then if it is in use anywhere (Connectors or AnyConnect) then it will have to be replaced with the new one.

**Step 4:** The key is active immediately. The email option below is only for the admin to have a backup of the key. **Note:** Once you navigate away from the page you’ll no longer see the complete string of the key (only the last 4 characters).

![Cisco Cloud Web Security](image)

**Figure 1.3**

**Step 5:** Copy the entire alphanumeric string in the **Authentication Key** field and record it in a document that will be backed up.

*Note: The second option is to create a group key by selecting **Group Key** under **Authentication**. To create a group key you may either use an existing directory group or you may create a custom group under → **Admin** → **Management** → **Groups***
**Step 6:** Click on the *Create Key* button which corresponds to the group for which you are creating a key.

*Notes: It is the same UI and process for creating a Company Key*

In an ASA deployment, when using IDFW with AD integration (CDA), groups should be defined in ScanCenter as Custom Groups in the format of DOMAIN\Group.
Deploy

Configure ASA connector

This document is intended to provide an overview of the deployment process. For more detailed information and troubleshooting, please refer to the Admin Guide.

Redirect web traffic

The following tutorial will show how to configure an ACL, policy maps, and class maps to identify HTTP and HTTPS traffic, and how to configure CWS to properly route this traffic to CWS on the ASA. This section will focus on using the command-line interface due to its simplicity.

Be sure to do the following before you begin:

- Ensure ASA version 9.0.4 or above, 9.1.5 or above
- Record primary and backup tower IP addresses
- Create Authentication license key
- View ASA training videos:
  - How to Configure ASA Connector
  - How to Configure User Identity for ASA Connector
  - How to Configure Whitelisting on ASA Connector

Command line Overview:

**Step 1:** Place all the configuration commands in a text editor.

**Step 2:** Configure the scansafe general-options. This is where the primary and backup Cloud Web Security proxies and the authentication license key are defined.

Next are the first two policy maps that define the service types to inspect: HTTP and HTTPS.
Two Access Control Lists will be created to identify the class of traffic to be sent to the Cloud Web Security service, one for HTTP traffic and the other for HTTPS traffic.

To identify the traffic the Cloud Web Security filtering should be enabled for, two class maps will be created: one for HTTP and one for HTTPS. For example configurations on how to whitelist traffic, see the Appendix.

A third policy map will be created to set actions and enable Cloud Web Security inspection on the class of traffic defined earlier.
Figure 2.5

Finally, a service policy will be created to activate the above policy map for the inside interface. However, if Cloud Web Security should be activated on all interfaces, the policy map `pmap-webtraffic` should be applied to internal interfaces.

Figure 2.6

**Step 3:** Verify the ASA is not filtering by browsing to `whoami.scansafe.net`. You should get the expected output ‘User is not currently using the service.’

**Step 4:** Enter enable mode and configure terminal mode. With a simple copy and paste, all of these configuration commands are immediately applied.

Figure 2.7

**Step 5:** Before writing to memory, test web browsing from a client by browsing to `whoami.scansafe.net`. Note that information on the client is returned, but not the logged on user. User identity will be explained in a later tutorial.

**Configure ACL whitelisting**

The concept of ACL whitelisting is to identify a source and/or destination host or network that should bypass Cloud Web Security filtering.

As you start using the Cloud Web Security solution, you may inevitably discover some mission critical web-based services are not compatible with a proxy. These would need to be whitelisted. Examples include a software update server hosted internally that synchronizes with a vendor’s software repository or an external financial service that performs IP authentication.
Reference video: Configure ACL whitelisting

**Step 1:** Verify that you are currently using the Cloud Web Security Service by browsing to whoami.scansafe.net. The website should generate the output below:

```plaintext
authUserName: CISCO\user
authenticated: true
cOMPANY Name: Cisco
connectorGuid: ABC012345AB
connectorVersion: AP_ASA-x.x(x)
countryCode: US
externalIp: 12.34.56.78
groupNames: []
internalIp: 1.2.3.4
logicalTowerNumber: 1782
staticGroupNames:
  - CISCO\Group
  - userName: CISCO\user
```

*Note: To demonstrate source whitelisting, we will configure the ACLs used to redirect traffic to Cloud Web Security Service to exempt the subnet our test machine is on.

**Step 2:** The subnet used for this lab is 192.168.159.0/24. Create an object for the subnet and name it SUBNET_159.

![Source Whitelisting.txt in Notepad](image)

*Note: In a real life scenario, there may be additional subnets or hosts that would need to be excluded from Cloud Web Security filtering.

**Step 3:** Create a group that will include the object SUBNET_159, and call it SOURCE_WHITELIST.
There are two ACLs that match the traffic for Cloud Web Security filtering: one for HTTP and one for HTTPS. To ensure proper whitelisting, an Access Control Entry (or ACE) will need to be added to both ACL’s referencing the SOURCE_WHITELIST group object.

*Note: The proper placement of the whitelisting ACE should occur before the ACE forwards traffic to the Cloud Web Security service. This can be achieved by using line 1 in the configuration command.

To demonstrate destination whitelisting, apply the aforementioned configuration to the ASA.

**Step 4:** From your test machine, browse to whoami.scansafe.net. As expected, you should see the message 'User is not currently using the service.'

Note that for the purposes of this tutorial access to www.cisco.com has been blocked in the Web Filtering Policy. This should only take effect when traffic is forwarded to the Cloud Web Security. Therefore, once the ACE has been created to accept traffic from www.cisco.com, this web request should no longer be blocked.
Step 5: Create an object for www.cisco.com and call it CISCO_FQDN.

As before, in a real life scenario there may be additional destinations to be excluded from Cloud Web Security filtering.

Step 6: Create a group that will include the object CISCO_FQDN and name it DESTINATION_WHITELIST.

Because of our two ACL that forward HTTP and HTTPS requests to the Cloud Web Security Service, an ACE should be created for each ACL that denies the particular traffic that matches the DESTINATION_WHITELIST group.
As before, the proper placement of the whitelisting ACE should occur before the ACE which forwards traffic to the Cloud Web Security Service. This can be achieved by using line 1 in the configuration command.

![Destination Whitelisting](image)

Figure 2.13

Applying this DESTINATION_WHITELIST to the ASA should allow the test machine access to [www.cisco.com](http://www.cisco.com).

**Configure user identity**

Before setting up user identity for the ASA Connector, formally known as identity firewall or IDFW, there are a few items to have on-hand.

Reference video: [Configure user identity](#)

**Be sure to have the following before you begin:**

- Service account for performing group lookups
- Configured Context Directory Agent (CDA). Please review CDA configuration instructions [here](#).
- One domain controller for group lookups
- NetBIOS domain name

A service account will be needed to map the web requestor's username to their IP address, and to perform a group lookup of the web requestor. This service account should be an active directory user belonging to either the domain admins or domain users group.

Since the ASA Connector does not have a built-in method for resolving IP addresses to usernames, it relies upon an external agent such as the Context Directory Agent (CDA). The installation and configuration of the CDA is out of scope for this tutorial, but note that it can use the same service account previously mentioned to map usernames to IP addresses. Consult this [link](#) for documentation.

At least one domain controller should be configured for group lookup requests. Multiple domain controllers can be configured for redundancy.

The NetBIOS domain name will be used in the user identity configuration. This is different from the DNS domain name, and can be found in the properties of the root domain object in Active Directory Users and Computers, or by running a gpresult on a client machine.

*Note: All four sections in the text editor in the screenshots below will need to be configured for complete user-identity and group membership discovery.*
Of these four sections there are two aaa-server groups to configure, one for domain controllers and another for the Context Directory Agent (CDA), a group of user-identity configurations, and additional user-identity monitor configurations for group discovery.

The first aaa-server group is for group lookups. It defines the domain controller, where to begin LDAP queries, whether or not to “walk the tree”, the type of directory, the port number LDAP queries will be performed on, the distinguished name of the service account, and the service account password.

The second aaa-server group configures the aaa-server group for CDA, allowing it to receive username to IP mapping updates from a CDA. The primary CDA is defined as the CDA host and shared secret if more than one CDA is used in the environment.

Next is a group of user-identity configurations which define how username to IP mappings and groups are handled on the ASA. When the domain is not explicitly defined for users or groups it defaults to the default domain. The inactive user timeout defines when a username to IP address mapping is no longer cached and requires an update from the CDA.

NetBIOS response fail defines the action to take when a client does not respond to a NetBIOS probe.
User not found tracking allows the ASA to cache erroneous users for better performance.

MAC address mismatch defines the action to take when a MAC address is found to be inconsistent with the mapped IP address, allowing the ASA to maintain an accurate username-to-IP-address mapping.

Active-user-database full-download specifies that the ASA will receive a complete user to IP address mapping database rather than on-demand updates, increasing overall performance.

Finally, for each group that is used in the web filtering policy, a complimentary monitor user-group configuration must be added. This specifies which groups the ASA will query for to determine if the web requestor is a member of said group.

![Figure 2.17](image1)

From the test machine, verify that you are using the Cloud Web Security service but user identity is still not configured by browsing to [whoami.scansafe.net](http://whoami.scansafe.net).

Then apply the user identity configuration to the ASA.

![Figure 2.18](image2)

Recall that the CDA receives logon notifications from a domain controller. Therefore, to ensure that the test machine will be properly resolved, log off and log back in.

Once the test machine is back up, browse to [whoami.scansafe.net](http://whoami.scansafe.net) again and see that the test account is properly resolved.

![Figure 2.19](image3)
Verify web redirection to the cloud

**Step 1:** From a client machine, browse to whoami.scansafe.net. If a message is displayed, “User is not currently using the service,” then the traffic is not redirected to the Cisco cloud. This can be useful in determining if the user is being resolved correctly, any groups being discovered, the internal/external IP of the user/location, and what connector is in use.

This is an example of a successful whoami.scansafe.net output:

```plaintext
authUserName: CISCO\user
authenticated: true
companyName: Cisco
connectorGuid: ABC012345AB
connectorVersion: AP_ASA-x.x(x)
countryCode: US
externalIp: 12.34.56.78
groupNames: []
internalIp: 1.2.3.4
logicalTowerNumber: 1782
staticGroupNames:
    - CISCO\Group
userName: CISCO\user
```

**Step 2:** From a client machine, browse to policytrace.scansafe.net and enter a URL to see how the web request is processed against the current web filtering policy.

**Step 3:** With SearchAhead enabled in ScanCenter (the CWS admin portal), browse to Google, Bing, or Yahoo and search for something. The SearchAhead data should be prepended to each search result in the form of a green, yellow, or red dot. Mouse over the dot to see what information is contained within.
## Appendix

### DESTINATION WHITELIST

<table>
<thead>
<tr>
<th>object network OBJECTNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>fqdn</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>object-group network OBJECTGROUPNAME</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>network-object object OBJECTNAME</th>
</tr>
</thead>
</table>

```
access-list web line 1 extended deny tcp any object-group OBJECTGROUPNAME eq www
access-list https line 1 extended deny tcp any object-group OBJECTGROUPNAME eq https
```

### SOURCE WHITELIST

<table>
<thead>
<tr>
<th>object network OBJECTNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>fqdn</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>object-group network OBJECTGROUPNAME</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>network-object object OBJECTNAME</th>
</tr>
</thead>
</table>

```
access-list web line 1 extended deny tcp object-group OBJECTGROUPNAME any eq www
access-list https line 1 extended deny tcp object-group OBJECTGROUPNAME any eq https
```

### SOURCE AND DESTINATION WHITELIST

```
access-list web line 1 extended deny tcp object-group OBJECTGROUPNAME object-group OBJECTGROUPNAME eq www
access-list https line 1 extended deny tcp object-group OBJECTGROUPNAME object-group OBJECTGROUPNAME eq https
```

---

Cisco CWS – ASA 5500 Deployment Guide

Appendix

### DESTINATION WHITELIST

<table>
<thead>
<tr>
<th>object network OBJECTNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>fqdn</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>object-group network OBJECTGROUPNAME</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>network-object object OBJECTNAME</th>
</tr>
</thead>
</table>

```
access-list web line 1 extended deny tcp any object-group OBJECTGROUPNAME eq www
access-list https line 1 extended deny tcp any object-group OBJECTGROUPNAME eq https
```

### SOURCE WHITELIST

<table>
<thead>
<tr>
<th>object network OBJECTNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>fqdn</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>object-group network OBJECTGROUPNAME</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>network-object object OBJECTNAME</th>
</tr>
</thead>
</table>

```
access-list web line 1 extended deny tcp object-group OBJECTGROUPNAME any eq www
access-list https line 1 extended deny tcp object-group OBJECTGROUPNAME any eq https
```

### SOURCE AND DESTINATION WHITELIST

```
access-list web line 1 extended deny tcp object-group OBJECTGROUPNAME object-group OBJECTGROUPNAME eq www
access-list https line 1 extended deny tcp object-group OBJECTGROUPNAME object-group OBJECTGROUPNAME eq https
```