Connect the Appliance to a Cisco Cloud Web Security Proxy

This topic contains the following sections:

How to Configure and Use Features in Cloud Connector Mode

Use of the features included in the Cloud Connector subset is the same as in standard mode, except as noted. See Comparison of Modes of Operation for additional information.

This topic links to locations within this documentation that provide information about some of the major features of the Web Security Appliance that are common to both standard mode and Cloud Web Security Connector mode. With the exception of Cloud Connector configuration settings and information about sending directory groups to the cloud, relevant information is in other locations throughout this document.

This topic includes information about configuring the Cloud Web Security Connector that is not applicable in standard mode.

This document does not include information about the Cisco Cloud Web Security product. Cisco Cloud Web Security documentation is available from http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

Deployment in Cloud Connector Mode

When you initially set up the appliance, you choose whether to deploy in Cloud Connector mode or standard mode. You can also run the System Setup Wizard on an appliance that is currently deployed in standard mode

to redeploy it in Cloud Connector mode, if you have the required licensing. Running the System Setup Wizard overwrites your existing configurations and deletes all existing data.

Deployment of the appliance is the same in both standard and Cloud Security mode except that on-site web proxy services and Layer-4 Traffic Monitor services are not available in Cloud Web Security Connector mode.

You can deploy the Cloud Web Security Connector in either explicit forward mode or in transparent mode.

To modify Cloud Connector settings after initial setup, select **Network** > **Cloud Connector**.

Related Topics

- Connect, Install, and Configure

Configuring the Cloud Connector

Before you begin

See Enabling Access to the Web Interface on Virtual Appliances.

Step 1 Access the Web Interface for the Web Security Appliance :

Enter the IPv4 address of the Web Security Appliance in an Internet browser.

The first time you run the System Setup Wizard, use the default IPv4 address:

`https://192.168.42.42:8443`

-or-

`http://192.168.42.42:8080`

where `192.168.42.42` is the default IPv4 address, and `8080` is the default admin port setting for HTTP, and `8443` is default admin port for HTTPS.

Step 2 Select **System Administration > System Setup Wizard**.

Step 3 Accept the terms of the license agreement.

Step 4 Click **Begin Setup**.

Step 5 Configure system settings:

Setting	Description
Default System Hostname	The fully-qualified hostname for the Web Security Appliance .
DNS Server(s)	The Internet root DNS servers for domain name service lookups. See also DNS Settings.
NTP Server	A server with which to synchronize the system clock. The default is time.ironport.com.
Time Zone	Sets the time zone on the appliance so that timestamps in message headers and log files are correct.

Step 6 Select **Cloud Web Security Connector** for the appliance mode.

Step 7 Configure Cloud Connector settings:

Setting	Description
Cloud Web Security Proxy Servers	The address of the Cloud Proxy Server (CPS), for example, proxy1743.scansafe.net.
Failure Handling	If AsyncOS fails to connect to a Cloud Web Security proxy, either **Connect directly** to the Internet or **Drop requests**.
Cloud Web Security Authorization Scheme	Method for authorizing transactions: • Web Security Appliance public facing IPv4 address • Authorization key included with each transaction. You can generate an authorization key within the Cisco Cloud Web Security Portal.

Step 8 Configure network interfaces and wiring:

Setting	Description
Ethernet Port	If you configure the M1 interface for management traffic only, you must configure the P1 interface for data traffic. However, you can configure the P1 interface even when the M1 interface is used for both management and data traffic.
IP Address	The IPv4 address to use to manage the Web Security Appliance .
Network Mask	The network mask to use when managing the Web Security Appliance on this network interface.
Hostname	The hostname to use when managing the Web Security Appliance on this network interface.

Step 9 Configure routes for Management and Data traffic:

Setting	Description
Default Gateway	The default gateway IPv4 address to use for the traffic through the Management and/or Data interface.
Name	A name used to identify the static route.
Internal Network	The IPv4 address for this route's destination on the network.
Internal Gateway	The gateway IPv4 address for this route. A route gateway must reside on the same subnet as the Management or Data interface on which it is configured.

Step 10 Configure transparent connection settings:

Note By default, the Cloud Connector is deployed in transparent mode. which requires a connection to a Layer-4 switch or a version 2 WCCP router.

Setting	Description
Layer-4 Switch or No Device	• The Web Security Appliance is connected to a layer 4 switch. or • You will deploy the Cloud Connector in explicit forward mode.
WCCP v2 Router	The Web Security Appliance is connected to a version 2 WCCP capable router. Note: A passphrase can contain up to seven characters and is optional.

Step 11 Configure administrative settings:

Setting	Description
Administrator Passphrase	A passphrase to access the Web Security Appliance . The passphrase must be six characters or more.
Email system alerts to	An email address to which the appliance sends alerts.
Send Email via SMTP Relay Host	(Optional) A hostname or address for an SMTP relay host that AsyncOS uses for sending system generated email messages. The default SMTP relay host is the mail servers listed in the MX record. The default port number is 25.
AutoSupport	The appliance can send system alerts and weekly status report to Cisco Customer Support.

Step 12 Review and install:

a) Review the installation.
b) Click **Previous** to go back and make changes.
c) Click **Install This Configuration** to continue with the information you provided.

What to do next

Related Topics

- Preventing Loss of Secure Data, on page 6
- Network Interfaces
- Configuring TCP/IP Traffic Routes
- Configuring Transparent Redirection
- Managing Alerts
- Configuring an SMTP Relay Host

Controlling Web Access Using Directory Groups in the Cloud

You can use Cisco Cloud Web Security to control web access based on directory groups. When traffic to Cisco Cloud Web Security is being routed through a Web Security Appliance in Cloud Connector mode, Cisco Cloud Web Security needs to receive the directory-group information with the transactions from the Cloud Connector so it can apply the group-based cloud policies.

Before you begin

Add an authentication realm to the Web Security Appliance configuration.

Step 1 Navigate to **Network** > **Cloud Connector**.

Step 2 In the **Cloud Policy Directory Groups** area, click **Edit Groups**.

Step 3 Select the User Groups and Machine Groups for which you have created Cloud Policies within Cisco Cloud Web Security.

Step 4 Click **Add**.

Step 5 Click **Done** and Commit your changes.

What to do next

Related information

- Authentication Realms

Bypassing the Cloud Proxy Server

Cloud routing policies allow you to route web traffic to either Cisco Cloud Web Security proxies or directly to the Internet based on these characteristics:

- **Identification Profile**
- Proxy Port
- Subnet
- URL Category
- User Agent

The process of creating cloud routing policies in Cloud Connector mode is identical to the process of creating routing policies using the standard mode.

Related Topics

- Creating a Policy

Partial Support for FTP and HTTPS in Cloud Connector Mode

The Web Security Appliance in Cloud Connector mode does not fully support FTP or HTTPS.

FTP

FTP is not supported by the Cloud Connector. AsyncOS drops native FTP traffic when the appliance is configured for Cloud Connector.

FTP over HTTP is supported in Cloud Connector mode.

HTTPS

The Cloud Connector does not support decryption. It passes HTTPS traffic without decrypting.

Because the Cloud Connector does not support decryption, AsyncOS generally does not have access to information in the client headers of HTTPS traffic. Therefore, AsyncOS generally cannot enforce routing policies that rely on information in encrypted headers. This is always the case for transparent HTTPS transactions. For example, for transparent HTTPS transactions, AsyncOS does not have access to the port number in the HTTPS client header and therefore it cannot match a routing policy based on port number. In this case, AsyncOS uses the default routing policy.

There are two exceptions for explicit HTTPS transactions. AsyncOS has access to the following information for explicit HTTPS transactions:

- URL
- Destination port number

For explicit HTTPS transactions, it is possible to match a routing policy based on URL or port number.

Preventing Loss of Secure Data

You can integrate the Cloud Connector with external Data Loss Prevention servers through **Network** > **External DLP Servers**.

Related Topics

- Prevent Loss of Sensitive Data

Viewing Group and User Names and IP Addresses

To view the configured group names, user names, and IP addresses, go to whoami.scansafe.net.

Subscribing to Cloud Connector Logs

The Cloud Connector Logs provides useful information for troubleshooting problems with the Cloud Connector, for example, authenticated users and groups, the Cloud header, and the authorization key.

Step 1 Navigate to **System Administration** > **Log Subscriptions**.

Step 2 Select **Cloud Connector Logs** from the **Log Type** menu.

Step 3 Type a name in the **Log Name** field.

Step 4 Set the log level.

Step 5 Submit and Commit your changes.

What to do next

Related Topics

- Monitor System Activity Through Logs

Identification Profiles and Authentication with Cloud Web Security Connector

The Cloud Web Security Connector supports basic authentication and NTLM. You can also bypass authentication for certain destinations.

In Cloud Connector mode, using an Active Directory realm, you can identify transaction requests as originating from specific machines. The Machine ID service is not available in standard mode.

With two exceptions, Authentication works the same throughout the Web Security Appliance , whether in standard configuration or Cloud Connector configuration. Exceptions:

- The Machine ID service is not available in standard mode.
- AsyncOS does not support Kerberos when the appliance is configured in Cloud Connector mode.

Note Identification Profiles based on User Agent or Destination URL are not supported for HTTPS traffic.

Related Topics

- Identifying Machines for Policy Application, on page 7
- Guest Access for Unauthenticated Users, on page 8
- Classify End-Users for Policy Application
- Overview of Acquire End-User Credentials

Identifying Machines for Policy Application

By enabling the Machine ID service, AsyncOS can apply policies based on the machine that made the transaction request rather than the authenticated user or IP address or some other identifier. AsyncOS uses NetBIOS to acquire the machine ID.

Note Be aware that the machine identity service is only available through Active Directory realms. If you do not have an Active Directory realm configured, this service is disabled.

Step 1 Select **Network** > **Machine ID Service**.

Step 2 Click **Enable and Edit Settings**.

Step 3 Configure Machine Identification settings:

Setting	Description
Enable NetBIOS for Machine Identification	Select to enable the machine identification service.
Realm	The Active Directory realm to use to identify the machine that is initiating the transaction request.
Failure Handling	If AsyncOS cannot identify the machine, should it drop the transaction or continue with policy matching?

Step 4 Submit and Commit your changes.

Guest Access for Unauthenticated Users

If the Web Security Appliance is configured to provide guest access for unauthenticated users, in Cloud Connector mode, AsyncOS assigns guest users to the group, __GUEST_GROUP__, and sends that information to Cisco Cloud Web Security. Use Identities to provide guest access to unauthenticated users. Use Cisco Cloud Web Security policies to control these guest users.

Related Topics

- Granting Guest Access After Failed Authentication