

Create Decryption Policies to Control HTTPS Traffic in AsyncOS 10.0 for Cisco Web Security Appliance



Contents

About This Document	3
Introduction to HTTPS Decryption	3
Enabling HTTPS Detection on the WSA	3
HTTPS Detection on the WSA in Action	4
WSA Certificate Use for HTTPS Decryption	5
Introduction	5
Certificate Overview	5
Root Certificates	6
Server Certificates	6

About This Document

This document is for Cisco engineers and customers who will deploy HTTPS decryption on the Cisco® Web Security Appliance (WSA) using AsyncOS® 10.0.

This document covers:

- Introduction to HTTPS decryption
- Enabling HTTPS detection on the Web Security Appliance
- HTTPS detection on the Web Security Appliance in action
- Web Security Appliance certificate use for HTTPS decryption

Introduction to HTTPS Decryption

To monitor and decrypt HTTPS traffic, you must enable the HTTPS proxy engine. When you enable the HTTPS proxy, you must configure what the appliance uses for a root certificate when it sends self-signed server certificates to the client applications on the network. You can upload a root certificate and key that your organization already has, or you can configure the appliance to generate a certificate and key with information you enter. This guide will walk you through the appliance generating a certificate you can use.

Before You Begin

When the HTTPS proxy is enabled, HTTPS-specific rules in access policies are disabled. The web proxy processes decrypted HTTPS traffic using rules for HTTP.

Note

The Cisco Cloud Connector does not support decryption. It passes HTTPS traffic without decrypting it to Cisco Cloud Web Security. HTTPS decryption is enabled on the Web Security Appliance only in standalone mode.

Decryption policies define the handling of HTTPS traffic within the web proxy. They define:

- When to decrypt HTTPS traffic
- How to handle requests that use invalid or revoked security certificates

Decryption policies can handle HTTPS traffic in the following ways. They can:

- Pass through encrypted traffic
- Decrypt traffic and apply content-based access policies defined for HTTP traffic. This process also makes malware scanning possible
- Drop the HTTPS connection
- Monitor the request (taking no final action) as the web proxy continues to evaluate the request against policies that may lead to a final drop, pass through, or decryption

Enabling HTTPS Detection on the WSA

Step 1. Choose **Security Services > HTTPS Proxy**. For the first use you will need to enable HTTPS proxy on the WSA. Click **Enable and Edit Settings**.



Step 2. Now select the checkbox **Enable HTTPS Proxy**. This will open a few options for you, which we will walk through.

Step 3. For this example we will use a generated certificate. Select the radio button **Use Generated Certificate and Key**.

Note

The WSA must have a root or intermediate certificate for the HTTPS proxy to work. There are a few options for getting a certificate on the box:

- For this guide you will generate the certificate and key on the WSA:
 - Click the **Generate New Certificate and Key** button.
 - Fill out the fields for the new certificate and key.
 - Click **Generate** when done.
- Generate a certificate and key and download a certificate signing request (CSR) to be signed by a certificate authority (CA):
 - Follow the steps for generating the certificate and key on the WSA above.

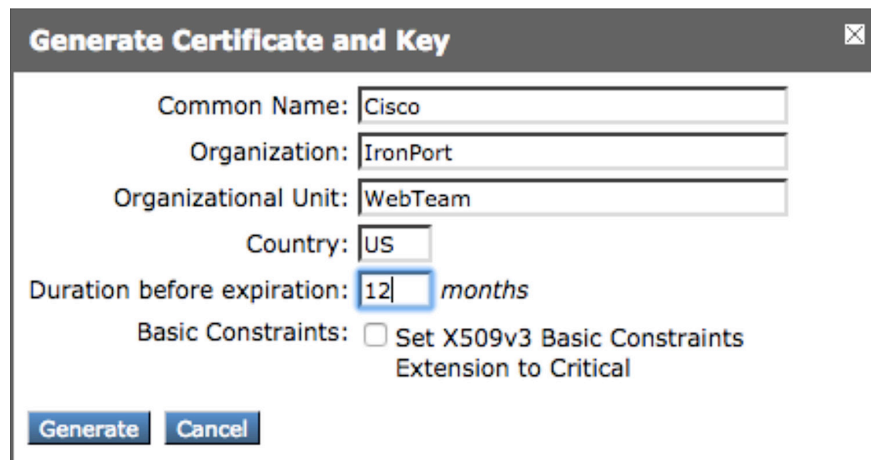
- Click the link **Download Certificate Signing Request** and save the file in PEM format.
- Take the file to your CA and have it signed.
- Click **Browse** under the section “Signed Certificate” to upload the signed certificate.

Note

The CA cannot be a third-party trusted CA, such as Verisign or Thawte, because they will not sign an intermediate or root certificate.

- Upload an existing certificate and key:
 - Select the box next to **Use Uploaded Certificate and Key**.
 - Select **Browse** to search for the certificate and key (as stated, a private key must be unencrypted).
 - Click **Upload Files** to upload the certificate and key.

Step 4. Continue from Step 3. Click **Generate New Certificate and Key**. You will need to populate the fields as shown in the example below. Click the **Generate** button.



Step 5. Click **Submit** and **Commit** all changes to save them.



Step 6. Select **Download Certificate**.

You can now take the certified PEM file and distribute it across your browsers. Remember, it needs to be imported into the trusted root certification authorities.

HTTPS Detection on the WSA in Action

After the Web Security Appliance assigns an HTTPS connection request to a Decryption Policy group, the connection request inherits the control settings of that policy group. The control settings of the Decryption Policy group determine whether the appliance decrypts, drops, or passes through the connection.

Step 1. Select **Web Security Manager > Decryption Policies**.

Step 2. You can configure the action to take on HTTPS requests for each predefined and custom URL category. Click the link under the URL Filtering column for the policy group you want to configure.

Note

If you want to block (with end-user notification) a particular URL category for HTTPS requests instead of dropping it (with no end-user notification), choose to decrypt that URL category in the Decryption Policy group. Then choose to block the same URL category in the Access Policy group. The URLs will be chosen in Step 3.

Step 3. Select the URL categories you would like to decrypt. In the following example, Social Networking is among those selected.

Category	Pass Through Select all	Monitor Select all	Decrypt Select all	Drop (?) Select all	Quota-Based (Unavailable)	Time-Based (Unavailable)
Nature		<input checked="" type="checkbox"/>			--	--
News	<input checked="" type="checkbox"/>				--	--
Non-governmental Organizations	<input checked="" type="checkbox"/>				--	--
Non-sexual Nudity			<input checked="" type="checkbox"/>		--	--
Online Communities		<input checked="" type="checkbox"/>			--	--
Online Storage and Backup	<input checked="" type="checkbox"/>				--	--
Online Trading	<input checked="" type="checkbox"/>				--	--
Organizational Email			<input checked="" type="checkbox"/>		--	--
Parked Domains			<input checked="" type="checkbox"/>		--	--
Peer File Transfer			<input checked="" type="checkbox"/>		--	--
Personal Sites	<input checked="" type="checkbox"/>				--	--
Photo Search and Images	<input checked="" type="checkbox"/>				--	--
Politics		<input checked="" type="checkbox"/>			--	--
Pornography			<input checked="" type="checkbox"/>		--	--
Professional Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			--	--
Real Estate		<input checked="" type="checkbox"/>			--	--
Reference	<input checked="" type="checkbox"/>				--	--
Religion			<input checked="" type="checkbox"/>		--	--
SaaS and B2B	<input checked="" type="checkbox"/>				--	--
Safe for Kids		<input checked="" type="checkbox"/>			--	--
Science and Technology		<input checked="" type="checkbox"/>			--	--
Search Engines and Portals	<input checked="" type="checkbox"/>				--	--
Sex Education		<input checked="" type="checkbox"/>			--	--
Shopping	<input checked="" type="checkbox"/>				--	--
Social Networking			<input checked="" type="checkbox"/>		--	--
Social Science		<input checked="" type="checkbox"/>			--	--
Society and Culture	<input checked="" type="checkbox"/>				--	--

Note

You can create decryption policies to handle HTTPS traffic in the following ways: pass through encrypted traffic, decrypt traffic, drop and monitor.

Step 4. When the URL categories are selected, click **Submit** and then **Commit** all changes to save them.

Step 5. Select **Web Security Manager > Access Policies** and select the policy you would like to modify. In the following example, Global Policy has been selected.

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	Office365 Identification Profile: O365 All identified users	(global policy)	Monitor: 1	(global policy)	(global policy)	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	
	Global Policy Identification Profile: All	No blocked items	Block: 4 Monitor: 75	Monitor: 365	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Disabled Anti-Malware Scanning: Enabled	

Step 6. Click the text within the URL Filtering cell.

Step 7. Select **Social Networking** as a category to **block**.

Category	Block Select all	Monitor Select all	Warn (?) Select all	Quota-Based (Unavailable)	Time-Based (Unavailable)
Real Estate		<input checked="" type="checkbox"/>		--	--
Reference		<input checked="" type="checkbox"/>		--	--
Religion		<input checked="" type="checkbox"/>		--	--
SaaS and B2B		<input checked="" type="checkbox"/>		--	--
Safe for Kids		<input checked="" type="checkbox"/>		--	--
Science and Technology		<input checked="" type="checkbox"/>		--	--
Search Engines and Portals		<input checked="" type="checkbox"/>		--	--
Sex Education		<input checked="" type="checkbox"/>		--	--
Shopping		<input checked="" type="checkbox"/>		--	--
Social Networking	<input checked="" type="checkbox"/>			--	--
Social Science		<input checked="" type="checkbox"/>		--	--
Society and Culture		<input checked="" type="checkbox"/>		--	--
Software Updates		<input checked="" type="checkbox"/>		--	--
Sports and Recreation		<input checked="" type="checkbox"/>		--	--
Streaming Audio		<input checked="" type="checkbox"/>		--	--

Step 8. Click **Submit** and **Commit** all changes.

Step 9. All social networking sites will now be decrypted and blocked.

WSA Certificate Use for HTTPS Decryption

Introduction

This section describes the type of certificate that should be used for HTTPS decryption on a Cisco Web Security Appliance.

Certificate Overview

The WSA has the ability to use a current certificate and private key with HTTPS decryption. However, not all X.509 certificates work.

There are two major types of certificates: server certificates and root certificates. All X.509 certificates contain a Basic Constraints field, which identifies the type of certificate:

- **Subject Type=End Entity** (server certificate)
- **Subject Type=CA** (root certificate)

Note: You must use a root certificate, also referred to as a certificate authority (CA) signing certificate, for HTTPS decryption on the WSA.

Root Certificates

A root certificate is specifically created for signing server certificates. You can create and operate your own CA and sign your own server certificates.

Note: Since a root certificate signs other certificates only, it cannot be used on a web server to perform HTTPS encryption and decryption.

The WSA must use a root certificate to actively generate server certificates for HTTPS decryption. Two options are available for root certificate use:

- You can generate a root certificate on the WSA. The WSA creates its own root certificate and private key, and it uses this key pair to sign server certificates.
- You can upload a current root certificate and its private key into the WSA. The Common Name (CN) field in a root certificate identifies the entity (typically a corporation name) that trusts any server certificates that contain its signature.

Note: Before a server certificate can be trusted, it must be signed by a root certificate that has a public key present in the web browser.

Server Certificates

A server certificate is specifically created to be used in HTTPS encryption and decryption and to verify the authenticity of a specific server. Server certificates are signed by a CA with use of the CA root certificate. Verisign and Thawte are well-known CAs.

Note: A server certificate cannot be used to sign other certificates. Therefore, HTTPS decryption does not work if a server certificate is installed on the WSA.

The CN field in a server certificate specifies the host for which the certificate is intended to be used. For example, <https://www.verisign.com> uses a server certificate with a CN of www.verisign.com.