

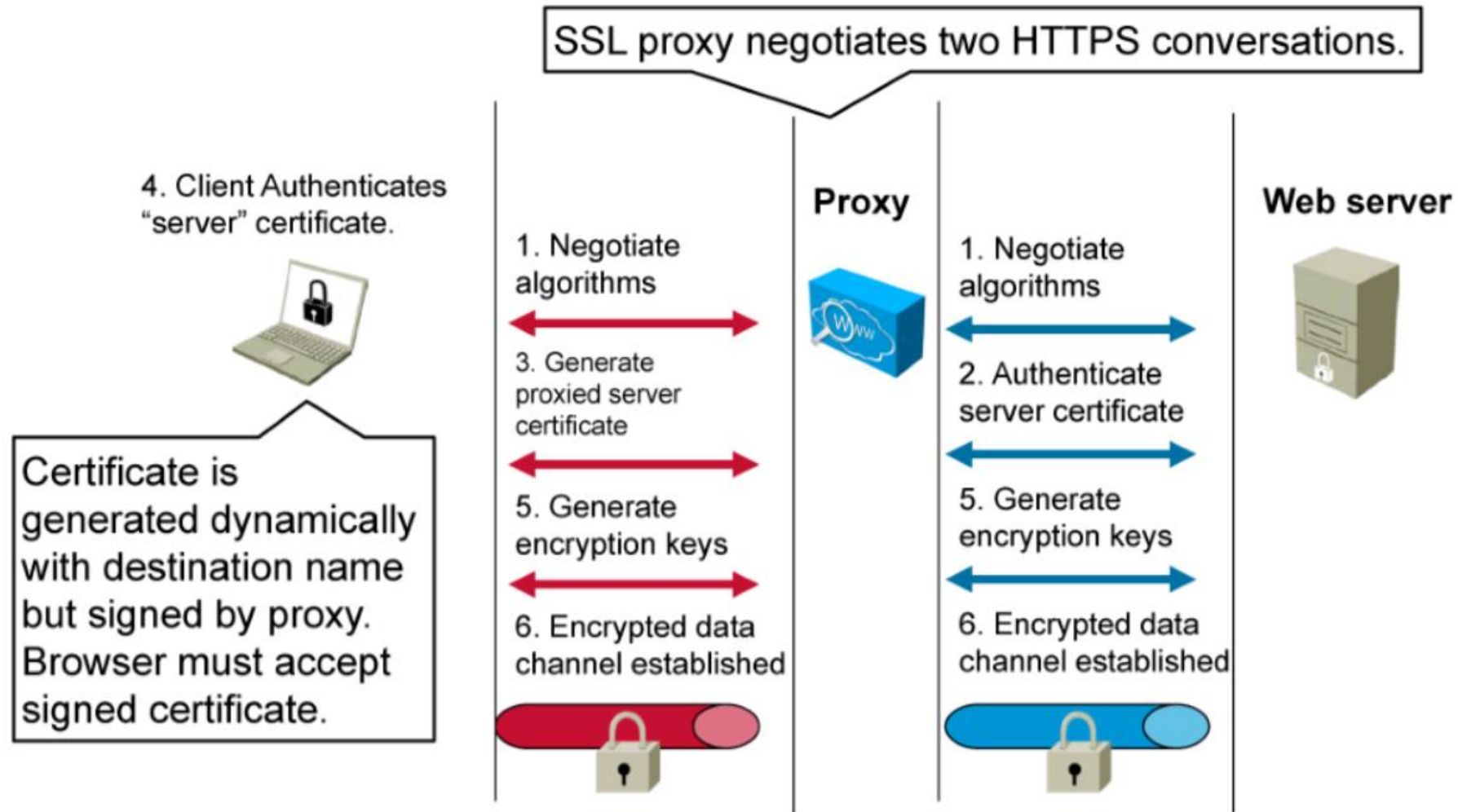


Configuring Cisco Web Security Appliance Decryption

Cisco Web Security Appliance

Ahmed Sultan
Senior Network Security Engineer
ahmedsultan.me/about

HTTPS Proxy Operations Overview



Enable HTTPS Proxy

The image shows the 'HTTPS Proxy Settings' configuration page. The main settings are as follows:

- Enable HTTPS Proxy:** ☒ (Annotated with a red box and arrow pointing to a summary box on the right).
- Transparent HTTPS Ports:** 443
- HTTPS Transparent Request:** ☒ Decrypt the HTTPS request for authentication purpose.
☐ Deny the HTTPS request.
Once the user is authenticated, subsequent HTTPS requests are subject to normal Decryption policies.
- Applications that Use HTTPS:** ☐ Enable decryption for enhanced application visibility and control.
- Root Certificate for Signing:** ☒ Use Generated Certificate and Key (Annotated with a red box and arrow pointing to the 'Generate New Certificate and Key' link).
No certificate has been generated.
☐ Use Uploaded Certificate and Key.
Certificate: [Browse]
Key: [Browse]
Private key must be unencrypted.
No certificate has been uploaded.
- Invalid Certificate Handling:**

Certificate Error	Drop
Expired	<input type="checkbox"/>
Mismatched Hostname	<input type="checkbox"/>
Unrecognized Root Authority	<input type="checkbox"/>
All other error types	<input type="checkbox"/>

No end-user notification will be provided for dropped HTTPS connections. Use this setting with caution. If the connection is not dropped, an equivalent certificate will be generated.

Summary Box (Top Right): HTTPS Proxy Settings. The HTTPS Proxy is currently disabled. [Enable and Edit Settings...](#) (Annotated with a red box and arrow pointing to the 'Enable HTTPS Proxy' checkbox).

Generate Certificate and Key Dialog (Bottom Right):

- Common Name: wsa.acme.com
- Organization: Acme
- Organizational Unit: IT
- Country: US
- Duration before expiration: 12 months
- Basic Constraints: ☐ Set X509v3 Basic Constraints Extension to Critical
- Buttons: Cancel, Generate (Annotated with a red box)

Invalid Destination Web Server Certificate Handling

Invalid Certificate Options				
Invalid Certificate Handling:	Certificate Error	Drop	Decrypt	Monitor
		Select all	Select all	Select all
	Expired Certificate			✓
	Mismatched Hostname			✓
	Unrecognized Root Authority / Issuer	✓		
	Invalid Signing Certificate	✓		
	Invalid Leaf Certificate	✓		
	All other error types	✓		
	No end-user notification will be provided for dropped HTTPS connections, unless the option to decrypt for end-user notification is enabled. If the connection is not dropped, an equivalent certificate will be generated.			

Navigate to **Security Services > HTTPS Proxy**

- Certificates can be valid or invalid (e.g. expired)
- You can configure how the WSA handles connections to servers with invalid certificates

Configure Decryption Policies

	Reporting	Web Security Manager	Security Services	Network	System Administration	
--	-----------	----------------------	-------------------	---------	-----------------------	--

Decryption Policies

Policies					
Add Policy...					
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
	Global Policy Identity: All	Monitor: 79	Enabled	Decrypt	



HTTPS Default Action: Global Policy

Policy Group Settings	
Default HTTPS Action: ?	<p><input checked="" type="radio"/> Decrypt</p> <p><input type="radio"/> Pass through without decrypting</p> <p><input type="radio"/> Drop Connection <i>No end-user notification will be provided for dropped HTTPS connections unless the option to decrypt for end-user notification is enabled (see Security Services > HTTPS Proxy).</i></p>
Cancel	Submit

Navigate to **Web Security Manager > Decryption Policies**


Configure Decryption Policies (Cont.)

Decryption Policies: Reputation Settings: Global Policy

Web Reputation Settings
Define Custom Web Reputation Settings ▾

Web Reputation Settings

Web Reputation Score

DROP -10.0 to -9.0	DECRYPT -8.9 to 5.9	PASS THROUGH 6.0 to 10.0
		
-10 -8 -6 -4 -2 0 2 4 6 8 +10		

Drop	Decrypt	Pass Through
The requested HTTPS connection is immediately dropped. No end-user notification will be provided. Use this setting with caution.	The HTTPS transaction will be decrypted for scanning and re-encrypted to ensure user privacy and security. The scanning defined in the applicable Web Access Policy will be performed.	The HTTPS request is passed through without decryption. No scanning will be performed.

Sites with No Score
Specify an action for sites that do not have a Web Reputation Score.
Sites with No Score: Monitor ▾

Cancel Submit