



List of Ciphers for AsyncOS 14.0.1 for Web Security Appliance

First Published: 2018-05-14

Last Modified: 2021-07-12

About Web Security Appliance

The Cisco Web Security Appliance intercepts and monitors Internet traffic and applies policies to help keep your internal network secure from malware, sensitive data loss, productivity loss, and other Internet-based threats.

Supported Ciphers

This section contains the list of supported ciphers (SSL and SSH) for AsyncOS for Web Security Appliance.

Port 8443 (Management Interface)

TLS 1.0	TLS 1.1	TLS 1.2
ECDHE-RSA-AES256-SHA - YES	ECDHE-RSA-AES256-SHA - YES	ECDHE-RSA-AES256-GCM-SHA384 - YES
DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-SHA - YES	ECDHE-RSA-AES256-SHA384 - YES
DHE-RSA-CAMELLIA256-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES	ECDHE-RSA-AES256-SHA - YES
AES256-SHA - YES	AES256-SHA - YES	DHE-RSA-AES256-GCM-SHA384 - YES
CAMELLIA256-SHA - YES	CAMELLIA256-SHA - YES	DHE-RSA-AES256-SHA256 - YES
ECDHE-RSA-DES-CBC3-SHA - YES	ECDHE-RSA-DES-CBC3-SHA - YES	DHE-RSA-AES256-SHA - YES
EDH-RSA-DES-CBC3-SHA - YES	EDH-RSA-DES-CBC3-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES
DES-CBC3-SHA - YES	DES-CBC3-SHA - YES	AES256-GCM-SHA384 - YES
ECDHE-RSA-AES128-SHA - YES	ECDHE-RSA-AES128-SHA - YES	AES256-SHA256 - YES
DHE-RSA-AES128-SHA - YES	DHE-RSA-AES128-SHA - YES	AES256-SHA - YES

TLS 1.0	TLS 1.1	TLS 1.2
DHE-RSA-SEED-SHA - YES	DHE-RSA-SEED-SHA - YES	CAMELLIA256-SHA - YES
DHE-RSA-CAMELLIA128-SHA - YES	DHE-RSA-CAMELLIA128-SHA - YES	ECDHE-RSA-DES-CBC3-SHA - YES
AES128-SHA - YES	AES128-SHA - YES	EDH-RSA-DES-CBC3-SHA - YES
SEED-SHA - YES	SEED-SHA - YES	DES-CBC3-SHA - YES
CAMELLIA128-SHA - YES	CAMELLIA128-SHA - YES	ECDHE-RSA-AES128-GCM-SHA256 - YES
		ECDHE-RSA-AES128-SHA256 - YES
		ECDHE-RSA-AES128-SHA - YES
		DHE-RSA-AES128-GCM-SHA256 - YES
		DHE-RSA-AES128-SHA256 - YES
		DHE-RSA-AES128-SHA - YES
		DHE-RSA-SEED-SHA - YES
		DHE-RSA-CAMELLIA128-SHA - YES
		AES128-GCM-SHA256 - YES
		AES128-SHA256 - YES
		AES128-SHA - YES
		SEED-SHA - YES
		CAMELLIA128-SHA - YES

Port 443 (SSL Port)

TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
ECDHE-RSA-AES128-SHA - YES	ECDHE-RSA-AES128-SHA - YES	DHE-RSA-AES256-GCM-SHA384 - YES	TLS_AES_128_GCM_SHA256 - YES
ECDHE-ECDSA-AES128-SHA - YES	ECDHE-ECDSA-AES128-SHA - YES	DHE-RSA-AES128-GCM-SHA256 - YES	TLS_CHACHA20_POLY1305_SHA256 - YES

TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-SHA 256 - YES	TLS_AES_256_GCM_SHA384 - YES
DHE-RSA-AES128-SHA - YES	DHE-RSA-AES128-SHA - YES	DHE-RSA-AES256-SHA - YES	
AES256-SHA - YES	AES256-SHA - YES	DHE-RSA-AES128-SHA - YES	
AES128-SHA - YES	AES128-SHA - YES	DHE-RSA-AES128-SHA 256 - YES	
		AES256-GCM-SHA384 - YES	
		AES256-SHA256 - YES	
		AES256-SHA - YES	
		AES128-GCM-SHA256 - YES	
		AES128-SHA256 - YES	
		AES128-SHA - YES	
		ECDHE-ECDSA-AES256-GCM-SHA384 - YES	
		ECDHE-ECDSA-CHACHA20-POLY1305 - YES	
		ECDHE-ECDSA-AES128-GCM-SHA256 - YES	
		ECDHE-ECDSA-AES256-SHA384 - YES	
		ECDHE-ECDSA-AES128-SHA256 - YES	
		ECDHE-ECDSA-AES128-CCM - YES	
		ECDHE-ECDSA-AES256-CCM - YES	
		ECDHE-RSA-AES256-GCM-SHA384 - YES	
		ECDHE-RSA-CHACHA20-POLY1305 - YES	

TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
		ECDHE-RSA-AES128-GCM-SHA256 - YES	
		ECDHE-RSA-AES256-SHA384 - YES	
		ECDHE-RSA-AES128-SHA256 - YES	
		ECDHE-RSA-AES128-SHA - YES	
Default Mode: DHE-RSA-AES128-SHA - YES AES128-SHA - YES	Default Mode: DHE-RSA-AES128-SHA - YES AES128-SHA - YES	Default Mode: AES256-GCM-SHA384 - YES AES256-SHA256 - YES DHE-RSA-AES128-SHA - YES AES128-GCM-SHA256 - YES AES128-SHA256 - YES AES128-SHA - YES	Default Mode: TLS_AES_256_GCM_SHA384 - YES
Note	AsyncOS 12.0.1 and later versions support ECDHE related ciphers for TLS 1.0, TLS 1.1, and TLS 1.2.		Note AsyncOS 12.0.1 and later versions support TLS 1.3.

Port 22 (SSH Port)

ssh2-enum-algos:

1. kex_algorithms (7):

- diffie-hellman-group-exchange\u0002sha256
- diffie-hellman-group-exchange\u0002sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

4. mac_algorithms (4):

- hmac-sha1
- hmac-ripemd160
- hmac-ripemd160@openssh.com
- umac-64@openssh.com

2. encryption_algorithms (8):

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- rijndael-cbc@lysator.liu.se
- aes128-ctr
- aes192-ctr
- aes256-ctr

3. server_host_key_algorithms (4):

- ssh-dss
- ssh-rsa
- rsa-sha2-512
- rsa-sha2-256

5. compression_algorithms (2):

- none
- zlib@openssh.com

Unsupported Ciphers

This section contains the list of unsupported ciphers.

Port 8443 (Management Interface)

SSL V 3.0	TLS 1.0
RC4-MD5	RC4-MD5
RC4-SHA	RC4-SHA

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2021 Cisco Systems, Inc. All rights reserved.