



List of Ciphers for AsyncOS 15.0 for Secure Web Appliance

First Published: 2023-05-11

Last Modified: 2023-05-12

About Secure Web Appliance

The Cisco Secure Web 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 Secure Web 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-AES128-SHA - YES	ECDHE-RSA-AES128-SHA - YES	DHE-RSA-AES256-SHA - YES
DHE-RSA-AES128-SHA - YES	DHE-RSA-AES128-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES
DHE-RSA-SEED-SHA - YES	DHE-RSA-SEED-SHA - YES	AES256-GCM-SHA384 - YES
DHE-RSA-CAMELLIA128-SHA - YES	DHE-RSA-CAMELLIA128-SHA - YES	AES256-SHA256 - YES
AES128-SHA - YES	AES128-SHA - YES	AES256-SHA - YES
SEED-SHA - YES	SEED-SHA - YES	CAMELLIA256-SHA - YES
CAMELLIA128-SHA - YES	CAMELLIA128-SHA - YES	ECDHE-RSA-AES128-GCM-SHA256 - YES
	RSA-PSK-AES256-CBC-SHA384 - YES	ECDHE-RSA-AES128-SHA - YES
		AES128-SHA - YES
		SEED-SHA - YES
		CAMELLIA128-SHA - YES

TLS 1.0	TLS 1.1	TLS 1.2
		ECDHE-ECDSA-AES256-GCM-SHA384 - YES
		ECDHE-ECDSA-AES128-GCM-SHA256 - YES
		ECDHE-ECDSA-AES128-SHA256 - YES
		DHE-PSK-AES256-GCM-SHA384 - YES

Port 443 (SSL Port)

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-GCM-SHA384 - YES	
ECDHE-RSA-AES128-SHA - YES	ECDHE-RSA-AES128-SHA - YES	DHE-RSA-AES128-GCM-SHA256 - YES	
ECDHE-ECDSA-AES128-SHA - YES	ECDHE-ECDSA-AES128-SHA - YES	DHE-RSA-AES256-SHA256 - YES	
AES256-SHA - YES	AES256-SHA - YES	DHE-RSA-AES128-SHA256 - YES	
AES128-SHA - YES	AES128-SHA - YES	DHE-RSA-AES256-SHA - YES	
	RSA-PSK-AES256-CBC-SHA384 - YES	DHE-RSA-AES256-CCM - YES	
	PSK-AES256-CBC-SHA384 - YES	ECDHE-RSA-AES256-GCM-SHA384 - YES	
	DHE-PSK-AES128-CBC-SHA256 - YES	ECDHE-RSA-AES128-SHA256 - YES	
		AES256-GCM-SHA384 - YES	
		AES128-GCM-SHA256 - YES	
		AES256-SHA256 - YES	
		AES128-SHA256 - YES	
		AES256-SHA - YES	
		AES128-SHA - YES	
		AES256-CCM - YES	
		AES128-CCM - YES	
		ECDHE-ECDSA-AES256-GCM-SHA384 - YES	
		ECDHE-ECDSA-AES128-GCM-SHA256 - YES	
		ECDHE-ECDSA-AES256-SHA384 - YES	

TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
		ECDHE-ECDSA-AES128-SHA256 - YES	
		ECDHE-ECDSA-AES128-SHA - YES	
		ECDHE-ECDSA-AES256-CCM - YES	
		ECDHE-ECDSA-AES128-CCM - YES	
Default Mode: ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA AES128-SHA DHE-RSA-AES128-SHA	Default Mode: ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA AES128-SHA DHE-RSA-AES128-SHA ECDHE-PSK-AES128-CBC-SHA256 ECDHE-PSK-AES128-CBC-SHA DHE-PSK-AES128-CBC-SHA256	Default Mode: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-RSA-AES128-SHA AES256-GCM-SHA384 AES128-GCM-SHA256 AES256-SHA256 AES128-SHA256 AES128-SHA DHE-RSA-AES128-SHA DHE-PSK-AES256-GCM-SHA384 ECDHE-PSK-CHACHA20-POLY1305 DHE-PSK-AES128-GCM-SHA256	Default Mode: TLS_CHACHA20_POLY1305_SHA256
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.
Note Default mode represents the supported ciphers with the “SSL Cipher String” that is configured in the Secure Web Appliance.			

Port 22 (SSH Port)

ssh2-enum-algos:

1. kex_algorithms (9):

- diffie-hellman-group14-sha1
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

2. encryption_algorithms

(9):

- 3des-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-cbc
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com

3. server_host_key_algorithms (14):

- ssh-ed25519
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- rsa-sha2-256
- ssh-rsa
- ssh-dss
- ssh-ed25519-cert-v01@openssh.com
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com
- ssh-rsa-cert-v01@openssh.com
- ssh-dss-cert-v01@openssh.com
- rsa-sha2-512

4. mac_algorithms (3):

- hmac-sha2-256
- hmac-sha1
- hmac-sha2-512

5.

compression_algorithms

(2):

- none
- zlib@openssh.com

Unsupported Ciphers

The following ciphers are not supported from the release SWA15.0 onwards with OpenSSL-1.1.1

TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305
DHE-RSA-CHACHA20-POLY1305

RSA-PSK-AES256-GCM-SHA384
DHE-PSK-AES256-GCM-SHA384
RSA-PSK-CHACHA20-POLY1305
DHE-PSK-CHACHA20-POLY1305
ECDHE-PSK-CHACHA20-POLY1305
PSK-AES256-GCM-SHA384
PSK-CHACHA20-POLY1305
RSA-PSK-AES128-GCM-SHA256
DHE-PSK-AES128-GCM-SHA256
PSK-AES128-GCM-SHA256
ECDHE-PSK-AES256-CBC-SHA384
RSA-PSK-AES256-CBC-SHA384
DHE-PSK-AES256-CBC-SHA384
PSK-AES256-CBC-SHA384
ECDHE-PSK-AES128-CBC-SHA256
ECDHE-PSK-AES128-CBC-SHA
RSA-PSK-AES128-CBC-SHA256
DHE-PSK-AES128-CBC-SHA256
RSA-PSK-AES128-CBC-SHA
DHE-PSK-AES128-CBC-SHA
PSK-AES128-CBC-SHA256

Port 8443 (Management Interface)

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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.

© 2023 Cisco Systems, Inc. All rights reserved.