List of Ciphers for AsyncOS 14.5 for Secure Web Appliance

First Published: 2022-04-11

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
		ECDHE-RSA-AES128-SHA256 - YES
		ECDHE-RSA-AES128-SHA - YES
		DHE-RSA-AES128-GCM-SHA256 - YES
		DHE-RSA-AES128-SHA256 - YES

TLS 1.0	TLS 1.1	TLS 1.2
		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
DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-GCM-SHA384 - YES	TLS_AES_256_GCM_SHA384 - YES
DHE-RSA-AES128-SHA - YES	DHE-RSA-AES128-SHA - YES	DHE-RSA-CHACHA20-POLY1305 - YES	TLS_CHACHA20_POLY1305_SHA256 - YES
ECDHE-RSA-AES128-SHA - YES	ECDHE-RSA-AES128-SHA - YES	DHE-RSA-AES128-GCM-SHA256 - YES	TLS_AES_128_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	
		DHE-RSA-AES128-SHA - YES	
		DHE-RSA-AES256-CCM - YES	
		DHE-RSA-AES128-CCM - YES	
		ECDHE-RSA-AES256-GCM-SHA384 - YES	
		ECDHE-RSA-CHACHA20-POLY1305 - YES	
		ECDHE-RSA-AES128-GCM-SHA256 - YES	
		ECDHE-RSA-AES256-SHA384 - YES	
		ECDHE-RSA-AES128-SHA256 - YES	
		ECDHE-RSA-AES128-SHA - YES	
		AES256-GCM-SHA384 - YES	
		AES128-GCM-SHA256 - YES	

TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
		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-CHACHA20-POLY1305 - YES	
		ECDHE-ECDSA-AES128-GCM-SHA256 - YES	
		ECDHE-ECDSA-AES256-SHA384 - YES	
		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	Default Mode: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-CHACHA20-POLY1305 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	Default Mode: TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256

TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
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-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- curve25519-sha256
- curve25519-sha256@libssh.org

2. encryption_algorithms (9):

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr
- 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

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