



AsyncOS 11.5 for Web Security Appliance の暗号リスト

公開日: 2018 年 3 月 14 日

目次

- [サポート対象の暗号方式 \(1 ページ\)](#)
- [サポート対象外の暗号方式 \(5 ページ\)](#)

サポート対象の暗号方式

このセクションには、AsyncOS 11.5 for Web セキュリティ アプライアンスのサポート対象の暗号 (SSL と SSH) のリストが含まれています。

ポート 8443 (管理インターフェイス)

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
ECDHE-RSA-AES256-SHA - YES	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	DHE-RSA-AES256-SHA - YES	ECDHE-RSA-AES256-SHA384 - YES
DHE-RSA-CAMELLIA256-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES	ECDHE-RSA-AES256-SHA - YES
AES256-SHA - YES	AES256-SHA - YES	AES256-SHA - YES	DHE-RSA-AES256-GCM-SHA384 - YES
CAMELLIA256-SHA - YES	CAMELLIA256-SHA - YES	CAMELLIA256-SHA - YES	DHE-RSA-AES256-SHA256 - YES



SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
ECDHE-RSA-DES-CB C3-SHA - YES	ECDHE-RSA-DES-CB C3-SHA - YES	ECDHE-RSA-DES-CB C3-SHA - YES	DHE-RSA-AES256-SH A - YES
EDH-RSA-DES-CBC3- SHA - YES	EDH-RSA-DES-CBC3- SHA - YES	EDH-RSA-DES-CBC3- SHA - YES	DHE-RSA-CAMELLI A256-SHA - YES
DES-CBC3-SHA - YES	DES-CBC3-SHA - YES	DES-CBC3-SHA - YES	AES256-GCM-SHA38 4 - YES
ECDHE-RSA-AES128- SHA - YES	ECDHE-RSA-AES128- SHA - YES	ECDHE-RSA-AES128- SHA - YES	AES256-SHA256 - YES
DHE-RSA-AES128-SH A - YES	DHE-RSA-AES128-SH A - YES	DHE-RSA-AES128-SH A - YES	AES256-SHA - YES
DHE-RSA-SEED-SHA - YES	DHE-RSA-SEED-SHA - YES	DHE-RSA-SEED-SHA - YES	CAMELLIA256-SHA - YES
DHE-RSA-CAMELLI A128-SHA - YES	DHE-RSA-CAMELLI A128-SHA - YES	DHE-RSA-CAMELLI A128-SHA - YES	ECDHE-RSA-DES-CB C3-SHA - YES
AES128-SHA - YES	AES128-SHA - YES	AES128-SHA - YES	EDH-RSA-DES-CBC3- SHA - YES
SEED-SHA - YES	SEED-SHA - YES	SEED-SHA - YES	DES-CBC3-SHA - YES
CAMELLIA128-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-G CM-SHA256 - YES
			DHE-RSA-AES128-SH A256 - YES
			DHE-RSA-AES128-SH A - YES
			DHE-RSA-SEED-SHA - YES
			DHE-RSA-CAMELLI A128-SHA - YES
			AES128-GCM-SHA25 6 - YES
			AES128-SHA256 - YES
			AES128-SHA - YES
			SEED-SHA - YES
			CAMELLIA128-SHA - YES

ポート 443(SSLポート)

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-GCM-SHA384 - YES
DHE-RSA-CAMELLIA256-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES	DHE-RSA-AES256-SHA256 - YES
ADH-AES256-SHA - YES	ADH-AES256-SHA - YES	ADH-AES256-SHA - YES	DHE-RSA-AES256-SHA - YES
ADH-CAMELLIA256-SHA - YES	ADH-CAMELLIA256-SHA - YES	ADH-CAMELLIA256-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES
AES256-SHA - YES	AES256-SHA - YES	AES256-SHA - YES	ADH-AES256-GCM-SHA384 - YES
CAMELLIA256-SHA - YES	CAMELLIA256-SHA - YES	CAMELLIA256-SHA - YES	ADH-AES256-SHA256 - YES
EDH-RSA-DES-CBC3-SHA - YES	EDH-RSA-DES-CBC3-SHA - YES	EDH-RSA-DES-CBC3-SHA - YES	ADH-AES256-SHA - YES
ADH-DES-CBC3-SHA - YES	ADH-DES-CBC3-SHA - YES	ADH-DES-CBC3-SHA - YES	ADH-CAMELLIA256-SHA - YES
DES-CBC3-SHA - YES	DES-CBC3-SHA - YES	DES-CBC3-SHA - YES	AES256-GCM-SHA384 - YES
DHE-RSA-AES128-SHA - YES	DHE-RSA-AES128-SHA - YES	DHE-RSA-AES128-SHA - YES	AES256-SHA256 - YES
DHE-RSA-SEED-SHA - YES	DHE-RSA-SEED-SHA - YES	DHE-RSA-SEED-SHA - YES	AES256-SHA - YES
DHE-RSA-CAMELLIA128-SHA - YES	DHE-RSA-CAMELLIA128-SHA - YES	DHE-RSA-CAMELLIA128-SHA - YES	CAMELLIA256-SHA - YES
ADH-AES128-SHA - YES	ADH-AES128-SHA - YES	ADH-AES128-SHA - YES	EDH-RSA-DES-CBC3-SHA - YES
ADH-SEED-SHA - YES	ADH-SEED-SHA - YES	ADH-SEED-SHA - YES	ADH-DES-CBC3-SHA - YES
ADH-CAMELLIA128-SHA - YES	ADH-CAMELLIA128-SHA - YES	ADH-CAMELLIA128-SHA - YES	DES-CBC3-SHA - YES
AES128-SHA - YES	AES128-SHA - YES	AES128-SHA - YES	DHE-RSA-AES128-GCM-SHA256 - YES
SEED-SHA - YES	SEED-SHA - YES	SEED-SHA - YES	DHE-RSA-AES128-SHA256 - YES
CAMELLIA128-SHA - YES	CAMELLIA128-SHA - YES	CAMELLIA128-SHA - YES	DHE-RSA-AES128-SHA - YES
			DHE-RSA-SEED-SHA - YES
			DHE-RSA-CAMELLIA128-SHA - YES

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
			ADH-AES128-GCM-SHA256 - YES
			ADH-AES128-SHA256 - YES
			ADH-AES128-SHA - YES
			ADH-SEED-SHA - YES
			ADH-CAMELLIA128-SHA - YES
			AES128-GCM-SHA256 - YES
			AES128-SHA256 - YES
			AES128-SHA - YES
			SEED-SHA - YES
			CAMELLIA128-SHA - YES
デフォルトモード: SSLV3が無効になっています	デフォルトモード: DHE-RSA-AES128-SHA - YES AES128-SHA - YES	デフォルトモード: DHE-RSA-AES128-SHA - YES AES128-SHA - YES	デフォルトモード: AES256-GCM-SHA384 - YES AES256-SHA256 - YES DHE-RSA-AES128-SHA - YES AES128-GCM-SHA256 - YES AES128-SHA256 - YES AES128-SHA - YES

ポート 22 (SSH ポート)

- ssh2-enum-algos:
- kex_algorithms: (7)
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- server_host_key_algorithms: (2)
- ssh-dss
- ssh-rsa
- encryption_algorithms: (8)
- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-cbc
- 3des-cbc
- aes192-cbc
- aes256-cbc
- rijndael-cbc@lysator.liu.se
- mac_algorithms: (7)
- hmac-md5
- hmac-sha1
- umac-64@openssh.com
- hmac-ripemd160
- hmac-ripemd160@openssh.com
- hmac-sha1-96
- hmac-md5-96
- compression_algorithms: (2)
- none
- _zlib@openssh.com

サポート対象外の暗号方式

このセクションには、サポート対象外の暗号のリストが含まれています。

ポート 8443 (管理インターフェイス)

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

ポート 22 (SSH ポート)

- arcfour256
- arcfour128
- blowfish-cbc
- arcfour

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: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owner. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図とその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2018 Cisco Systems, Inc. All rights reserved.