تفاصيل قوة تشفير SSL

المحتويات

المقدمة
تفاصيل قوة تشفير SSL
كيفية التحقق من تشفير TLSv1.2
كيفية التحقق من شفرات SSLv3
كيفية التحقق من التشفير المنخفض
كيفية التحقق من التشفير المتوسط
كيفية التحقق من التشفير العالي
معلومات ذات صلة

المقدمة

يصف هذا وثيقة كيف أن يشاهد ال SSL تشفير أن يكون يتوفر للاستخدام ومدعوم على ال cisco بريد إلكتروني أمن تطبيق (ESA).

تفاصيل قوة تشفير SSL

يمكن ملاحظة شفرات SSL المتوفرة للاستخدام والمدعومة في أي وقت عن طريق تشغيل ما يلي من واجهة سطر الأوامر: **sslconfig > التحقق**

عند المطالبة "أدخل تشفير SSL الذي تريد التحقق منه"، اضغط على مفتاح الرجوع لمغادرة هذا الحقل فارغا وعرض جميع الشفرات.

ecdhe-rsa-aes256-gcm-sha384	TLSv1.2	Kx=ECDH	AU=RSA	ENC=AESGCM(256)	Mac=AEAD
ecdhe-ecdsa-aes256-gcm-sha384	TLSv1.2	Kx=ECDH	AU=ECDSA	ENC=AESGCM(256)	Mac=AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	Kx=ECDH	AU=RSA	ENC=AES(256)	Mac=SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	Kx=ECDH	AU=ECDSA	ENC=AES(256)	Mac=SHA384
ECDHE-RSA-AES256-SHA	SSLv3	Kx=ECDH	AU=RSA	ENC=AES(256)	Mac=SHA1
ECDHE-	SSLv3	Kx=ECDH	AU=ECD	ENC=AE	Mac=SHA1

ECDSA-AES256-SHA			SA	(S(256	
SRP-DSS-AES-256-CBC-SHA	SSLv3	kx=srp	AU=DSS	ENC=AE(S(256	Mac=SHA1
SRP-RSA-AES-256-CBC-SHA	SSLv3	kx=srp	AU=RSA	ENC=AE(S(256	Mac=SHA1
SRP-AES-256-CBC-SHA	SSLv3	kx=srp	AU=SRP	ENC=AE(S(256	Mac=SHA1
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=dh	AU=DSS	ENC=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=dh	AU=RSA	ENC=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-SHA256	TLSv1.2	Kx=dh	AU=RSA	ENC=AE(S(256	Mac=SHA256
DHE-DSS-AES256-SHA256	TLSv1.2	Kx=dh	AU=DSS	ENC=AE(S(256	Mac=SHA256
DHE-RSA-AES256-SHA	SSLv3	Kx=dh	AU=RSA	ENC=AE(S(256	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3	Kx=dh	AU=DSS	ENC=AE(S(256	Mac=SHA1
DHE-RSA-Camellia256-SHA	SSLv3	Kx=dh	AU=RSA	ENC=Camellia(256)	Mac=SHA1
DHE-DSS-Camellia256-SHA	SSLv3	Kx=dh	AU=DSS	ENC=Camellia(256)	Mac=SHA1
AES256-GCM-SHA384	TLSv1.2	KX=RSA	AU=RSA	ENC=AESGCM(256)	Mac=AEAD
الطراز AES256-SHA256	TLSv1.2	KX=RSA	AU=RSA	ENC=AE(S(256	Mac=SHA256
الطراز AES256-SHA	SSLv3	KX=RSA	AU=RSA	ENC=AE(S(256	Mac=SHA1
كاميليا 256-شا	SSLv3	KX=RSA	AU=RSA	ENC=Camellia(256)	Mac=SHA1
PSK-AES256-CBC-SHA	SSLv3	KX=PSK	أو=psk	ENC=AE(S(256	Mac=SHA1

Mac=AEAD	ENC=AESGCM(128)	AU=RSA	Kx=ECDH	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256
Mac=AEAD	ENC=AESGCM(128)	AU=ECDSA	Kx=ECDH	TLSv1.2	ecdhe-ecdsa-aes128-gcm-sha256
Mac=SHA256	ENC=AES(128	AU=RSA	Kx=ECDH	TLSv1.2	ECDHE-RSA-AES128-SHA256
Mac=SHA256	ENC=AES(128	AU=ECDSA	Kx=ECDH	TLSv1.2	ecdhe-ecdsa-aes128-sha256
Mac=SHA1	ENC=AES(128	AU=RSA	Kx=ECDH	SSLv3	ECDHE-RSA-AES128-SHA
Mac=SHA1	ENC=AES(128	AU=ECDSA	Kx=ECDH	SSLv3	ECDHE-ECDSA-AES128-SHA
Mac=SHA1	ENC=AES(128	AU=DSS	kx=srp	SSLv3	SRP-DSS-AES-128-CBC-SHA
Mac=SHA1	ENC=AES(128	AU=RSA	kx=srp	SSLv3	SRP-RSA-AES-128-CBC-SHA
Mac=SHA1	ENC=AES(128	AU=SRP	kx=srp	SSLv3	SRP-AES-128-CBC-SHA
Mac=AEAD	ENC=AESGCM(128)	AU=DSS	Kx=dh	TLSv1.2	DHE-DSS-AES128-GCM-SHA256
Mac=AEAD	ENC=AESGCM(128)	AU=RSA	Kx=dh	TLSv1.2	DHE-RSA-AES128-GCM-SHA256
Mac=SHA256	ENC=AES(128	AU=RSA	Kx=dh	TLSv1.2	DHE-RSA-AES128-SHA256
Mac=SHA256	ENC=AES(128	AU=DSS	Kx=dh	TLSv1.2	DHE-DSS-AES128-SHA256
Mac=SHA1	ENC=AES(128	AU=RSA	Kx=dh	SSLv3	DHE-RSA-AES128-SHA

معيار

DHE-DSS-AES128-SHA	SSLv3	Kx=dh	AU=DSS	ENC=AES(128)	Mac=SHA1
DHE-RSA-Seed-SHA	SSLv3	Kx=dh	AU=RSA	ENC=SEED(128)	Mac=SHA1
DHE-DSS-Seed-SHA	SSLv3	Kx=dh	AU=DSS	ENC=SEED(128)	Mac=SHA1
DHE-RSA-Camellia128-SHA	SSLv3	Kx=dh	AU=RSA	ENC=Camellia(128)	Mac=SHA1
DHE-DSS-Camellia128-SHA	SSLv3	Kx=dh	AU=DSS	ENC=Camellia(128)	Mac=SHA1
الطراز AES128-GCM-SHA256	TLSv1.2	KX=RSA	AU=RSA	ENC=AESGCM(128)	Mac=AEAD
الطراز AES128-SHA256	TLSv1.2	KX=RSA	AU=RSA	ENC=AES(128)	Mac=SHA256
الطراز AES128-SHA	SSLv3	KX=RSA	AU=RSA	ENC=AES(128)	Mac=SHA1
بذرة شعاع	SSLv3	KX=RSA	AU=RSA	ENC=SEED(128)	Mac=SHA1
كاميليا 128-شا	SSLv3	KX=RSA	AU=RSA	ENC=Camellia(128)	Mac=SHA1
IDEA-CBC-SHA	SSLv3	KX=RSA	AU=RSA	ENC=IDEA(128)	Mac=SHA1
PSK-AES128-CBC-SHA	SSLv3	KX=PSK	أو=psk	ENC=AES(128)	Mac=SHA1
ECDHE-RSA-RC4-SHA	SSLv3	Kx=ECDH	AU=RSA	ENC=RC4(128)	Mac=SHA1
ECDHE-ECDSA-RC4-SHA	SSLv3	Kx=ECDH	AU=ECDSA	ENC=RC4(128)	Mac=SHA1
التعاون الإقليمي 4-شاو	SSLv3	KX=RSA	AU=RSA	ENC=RC4(128)	Mac=SHA1
RC4-MD5	SSLv3	KX=RSA	AU=RSA	ENC=RC4(128)	Mac=MD5
PSK-RC4-SHA	SSLv3	KX=PSK	أو=psk	ENC=RC4(128)	Mac=SHA1
ECDHE-RSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	AU=RSA	ENC=3DES(168)	Mac=SHA1
ECDHE-ECDSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	AU=ECDSA	ENC=3DES(168)	Mac=SHA1

SRP-DSS-3DES-EDE-CBC-SHA	SSLv3	kx=srp	AU=DSS	ENC=3DE(S(168	Mac=SHA1
SRP-RSA-3DES-EDE-CBC-SHA	SSLv3	kx=srp	AU=RSA	ENC=3DE(S(168	Mac=SHA1
SRP-3DES-EDE-CBC-SHA	SSLv3	kx=srp	AU=SRP	ENC=3DE(S(168	Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3	Kx=dh	AU=RSA	ENC=3DE(S(168	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3	Kx=dh	AU=DSS	ENC=3DE(S(168	Mac=SHA1
DES-CBC3-SHA	SSLv3	KX=RSA	AU=RSA	ENC=3DE(S(168	Mac=SHA1
PSK-3DES-EDE-CBC-SHA	SSLv3	KX=PSK	أو=psk	ENC=3DE(S(168	Mac=SHA1
EDH-RSA-DES-CBC-SHA	SSLv3	Kx=dh	AU=RSA	ENC=DE(S(56	Mac=SHA1
EDH-DSS-DES-CBC-SHA	SSLv3	Kx=dh	AU=DSS	ENC=DE(S(56	Mac=SHA1
دي سي بي سي-شا	SSLv3	KX=RSA	AU=RSA	ENC=DE(S(56	Mac=SHA1

كيفية التحقق من تشفير TLSv1.2

من موقع **sslconfig > التحقق** CLI القائمة، أستخدم "TLSv1.2" عند السؤال SSL تشفير للتحقق:

```
.Enter the ssl cipher you want to verify
TLSv1.2 <[]
```

```
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-DSS-AES256-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(256) Mac=SHA256
ADH-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=None Enc=AESGCM(256) Mac=AEAD
ADH-AES256-SHA256 TLSv1.2 Kx=DH Au=None Enc=AES(256) Mac=SHA256
AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
```

```
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
   DHE-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(128) Mac=AEAD
   DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
        DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
        DHE-DSS-AES128-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(128) Mac=SHA256
     ADH-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=None Enc=AESGCM(128) Mac=AEAD
          ADH-AES128-SHA256 TLSv1.2 Kx=DH Au=None Enc=AES(128) Mac=SHA256
       AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
            AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
                  NULL-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=None Mac=SHA256
```

كيفية التحقق من شفرات SSLv3

من موقع **sslconfig > التحقق** CLI القائمة، أستخدم "SSLv3" عند السؤال SSL تشفير للتحقق:

```
                                                .Enter the ssl cipher you want to verify
                                                                              SSLv3 <[]

                  ECDHE-RSA-AES256-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
                ECDHE-ECDSA-AES256-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1
                  SRP-DSS-AES-256-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=AES(256) Mac=SHA1
                  SRP-RSA-AES-256-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=AES(256) Mac=SHA1
                      SRP-AES-256-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=AES(256) Mac=SHA1
                        DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
                        DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
               DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
               DHE-DSS-CAMELLIA256-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(256) Mac=SHA1
                          ADH-AES256-SHA SSLv3 Kx=DH Au=None Enc=AES(256) Mac=SHA1
             ADH-CAMELLIA256-SHA SSLv3 Kx=DH Au=None Enc=Camellia(256) Mac=SHA1
                           AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
                CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
                  PSK-AES256-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=AES(256) Mac=SHA1
                ECDHE-RSA-AES128-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
              ECDHE-ECDSA-AES128-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
                SRP-DSS-AES-128-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=AES(128) Mac=SHA1
                SRP-RSA-AES-128-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=AES(128) Mac=SHA1
                    SRP-AES-128-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=AES(128) Mac=SHA1
                      DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
                      DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
                       DHE-RSA-SEED-SHA SSLv3 Kx=DH Au=RSA Enc=SEED(128) Mac=SHA1
                       DHE-DSS-SEED-SHA SSLv3 Kx=DH Au=DSS Enc=SEED(128) Mac=SHA1
               DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
               DHE-DSS-CAMELLIA128-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(128) Mac=SHA1
                          ADH-AES128-SHA SSLv3 Kx=DH Au=None Enc=AES(128) Mac=SHA1
                         ADH-SEED-SHA SSLv3 Kx=DH Au=None Enc=SEED(128) Mac=SHA1
             ADH-CAMELLIA128-SHA SSLv3 Kx=DH Au=None Enc=Camellia(128) Mac=SHA1
                           AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
                          SEED-SHA SSLv3 Kx=RSA Au=RSA Enc=SEED(128) Mac=SHA1
                CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
                         IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
                  PSK-AES128-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=AES(128) Mac=SHA1
                  ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
              ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
                           ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
                              RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
                               RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
                          PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
             ECDHE-RSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=RSA Enc=3DES(168) Mac=SHA1
           ECDHE-ECDSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=3DES(168) Mac=SHA1
             SRP-DSS-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=3DES(168) Mac=SHA1
             SRP-RSA-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=3DES(168) Mac=SHA1
                 SRP-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=3DES(168) Mac=SHA1
```

```
EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1
ADH-DES-CBC3-SHA SSLv3 Kx=DH Au=None Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
PSK-3DES-EDE-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=3DES(168) Mac=SHA1
EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH Au=DSS Enc=DES(56) Mac=SHA1
ADH-DES-CBC-SHA SSLv3 Kx=DH Au=None Enc=DES(56) Mac=SHA1
DES-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
EXP-EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH(512) Au=DSS Enc=DES(40) Mac=SHA1 export
EXP-ADH-DES-CBC-SHA SSLv3 Kx=DH(512) Au=None Enc=DES(40) Mac=SHA1 export
EXP-DES-CBC-SHA SSLv3 Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-ADH-RC4-MD5 SSLv3 Kx=DH(512) Au=None Enc=RC4(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
ECDHE-RSA-NULL-SHA SSLv3 Kx=ECDH Au=RSA Enc=None Mac=SHA1
ECDHE-ECDSA-NULL-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=None Mac=SHA1
NULL-SHA SSLv3 Kx=RSA Au=RSA Enc=None Mac=SHA1
NULL-MD5 SSLv3 Kx=RSA Au=RSA Enc=None Mac=MD5
```

كيفية التحقق من التشفير المنخفض

من **sslconfig > التحقق من** قائمة CLI، أستخدم "منخفض" عند سؤالك عن تشفير SSL الذي سيتحقق:

```
.Enter the ssl cipher you want to verify
LOW <[]

EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH Au=DSS Enc=DES(56) Mac=SHA1
ADH-DES-CBC-SHA SSLv3 Kx=DH Au=None Enc=DES(56) Mac=SHA1
DES-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
DES-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5
```

كيفية التحقق من التشفير المتوسط

من موقع **sslconfig > التحقق** قائمة واجهة سطر الأوامر (CLI)، أستخدم "متوسط" عند سؤالك عن تشفير SSL الذي سيتم التحقق منه:

```
.Enter the ssl cipher you want to verify
MEDIUM <[]

DHE-RSA-SEED-SHA SSLv3 Kx=DH Au=RSA Enc=SEED(128) Mac=SHA1
DHE-DSS-SEED-SHA SSLv3 Kx=DH Au=DSS Enc=SEED(128) Mac=SHA1
ADH-SEED-SHA SSLv3 Kx=DH Au=None Enc=SEED(128) Mac=SHA1
SEED-SHA SSLv3 Kx=RSA Au=RSA Enc=SEED(128) Mac=SHA1
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
```

كيفية التحقق من التشفير العالي

من موقع **sslconfig > التحقق** قائمة واجهة سطر الأوامر (CLI)، أستخدم "High" عند سؤالك عن تشفير SSL الذي

سيتم التحقق منه:

```
.Enter the ssl cipher you want to verify
HIGH <[]

    ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
  ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
       ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
     ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
                ECDHE-RSA-AES256-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
              ECDHE-ECDSA-AES256-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1
                SRP-DSS-AES-256-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=AES(256) Mac=SHA1
                SRP-RSA-AES-256-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=AES(256) Mac=SHA1
                   SRP-AES-256-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=AES(256) Mac=SHA1
          DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(256) Mac=AEAD
          DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
               DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
               DHE-DSS-AES256-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(256) Mac=SHA256
                      DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
                      DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
            DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
            DHE-DSS-CAMELLIA256-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(256) Mac=SHA1
             ADH-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=None Enc=AESGCM(256) Mac=AEAD
                  ADH-AES256-SHA256 TLSv1.2 Kx=DH Au=None Enc=AES(256) Mac=SHA256
                        ADH-AES256-SHA SSLv3 Kx=DH Au=None Enc=AES(256) Mac=SHA1
               ADH-CAMELLIA256-SHA SSLv3 Kx=DH Au=None Enc=Camellia(256) Mac=SHA1
                AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
                     AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
                           AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
                    CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
                     PSK-AES256-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=AES(256) Mac=SHA1
    ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
  ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
       ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
     ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
                ECDHE-RSA-AES128-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
              ECDHE-ECDSA-AES128-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
                SRP-DSS-AES-128-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=AES(128) Mac=SHA1
                SRP-RSA-AES-128-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=AES(128) Mac=SHA1
                   SRP-AES-128-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=AES(128) Mac=SHA1
          DHE-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(128) Mac=AEAD
          DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
               DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
               DHE-DSS-AES128-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(128) Mac=SHA256
                      DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
                      DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
            DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
            DHE-DSS-CAMELLIA128-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(128) Mac=SHA1
             ADH-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=None Enc=AESGCM(128) Mac=AEAD
                  ADH-AES128-SHA256 TLSv1.2 Kx=DH Au=None Enc=AES(128) Mac=SHA256
                        ADH-AES128-SHA SSLv3 Kx=DH Au=None Enc=AES(128) Mac=SHA1
               ADH-CAMELLIA128-SHA SSLv3 Kx=DH Au=None Enc=Camellia(128) Mac=SHA1
                AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
                     AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
                           AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
                    CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
                     PSK-AES128-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=AES(128) Mac=SHA1
               ECDHE-RSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=RSA Enc=3DES(168) Mac=SHA1
            ECDHE-ECDSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=3DES(168) Mac=SHA1
               SRP-DSS-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=3DES(168) Mac=SHA1
               SRP-RSA-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=3DES(168) Mac=SHA1
                  SRP-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=3DES(168) Mac=SHA1
```

```
EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1
   ADH-DES-CBC3-SHA SSLv3 Kx=DH Au=None Enc=3DES(168) Mac=SHA1
       DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
        DES-CBC3-MD5 SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5
PSK-3DES-EDE-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=3DES(168) Mac=SHA1
```

معلومات ذات صلة

- منع التفاوض على التشفير الفارغ أو المجهول على ESA و SMA
- تبديل الطرق والشفرات المستخدمة مع SSL/TLS على ESA

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).