

Unterstützte SSL/TLS-Verschlüsselungssammlungen

Veröffentlicht: 2023-09-30

Das ExtraHop-System kann SSL/TLS-Verkehr entschlüsseln, der mit PFS- oder RSA-Cipher Suites verschlüsselt wurde. Alle unterstützten Cipher Suites können entschlüsselt werden, indem der Session Key Forwarder auf einem Server installiert und das ExtraHop-System konfiguriert wird.

Cipher Suites for RSA können den Datenverkehr auch mit einem Zertifikat und einem privaten Schlüssel entschlüsseln – mit oder ohne Weiterleitung von Sitzungsschlüsseln.

Entschlüsselungsmethoden

Die folgende Tabelle enthält eine Liste der Cipher Suites, die das ExtraHop-System unterstützt [entschlüsseln](#) zusammen mit den unterstützten Entschlüsselungsoptionen.

- **PFS + GPP:** Das ExtraHop-System kann diese Cipher Suites mit Sitzungsschlüsselweiterleitung entschlüsseln und [Zuordnung von globalen Protokoll zu Anschlüssen](#)
- **PFS + Zertifikat:** Das ExtraHop-System kann diese Cipher Suites mit der Weiterleitung von Sitzungsschlüsseln entschlüsseln und [Zertifikat und privater Schlüssel](#)
- **RSA+-Zertifikat:** Das ExtraHop-System kann diese Cipher Suites ohne Weiterleitung des Sitzungsschlüssels entschlüsseln, sofern Sie das hochgeladen haben [Zertifikat und privater Schlüssel](#)

Hex-Wert	Vorname (IANA)	Name (OpenSSL)	Unterstützte Entschlüsselung
0 x 04	TLS_RSA_MIT_RC4_128_MD5	TLS_RSA_WITH_RC4_128_MD5	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 05	TLS_RSA_MIT_RC4_128_SHA	TLS_RSA_WITH_RC4_128_SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	PFS + GPP PFS + Zertifikat
0x2F	TLS_RSA_MIT_AES_128_CBC_SHA	TLS_RSA_WITH_AES_128_CBC_SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 33	TLS_DHE_RSA_MIT_AES_128_CBC_SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	PFS + GPP PFS + Zertifikat
0 x 35	TLS_RSA_MIT_AES_256_CBC_SHA	TLS_RSA_WITH_AES_256_CBC_SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 39	TLS_DHE_RSA_MIT_AES_256_CBC_SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	PFS + GPP PFS + Zertifikat
0x3C	TLS_RSA_MIT_AES_128_CBC_SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat

Hex-Wert	Vorname (IANA)	Name (OpenSSL)	Unterstützte Entschlüsselung
0x3D	TLS_RSA_MIT_AES_256_CBC_SHA256	TLS_RSA_MIT_AES_256_CBC_SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 67	TLS_DHE_RSA_MIT_AES_128_CBC_SHA256	TLS_DHE_RSA_MIT_AES_128_CBC_SHA256	PFS + GPP PFS + Zertifikat
0 x 6 B	TLS_DHE_RSA_MIT_AES_256_CBC_SHA256	TLS_DHE_RSA_MIT_AES_256_CBC_SHA256	PFS + GPP PFS + Zertifikat
0 x 9 C	TLS_RSA_MIT_AES_128_GCM_SHA256	TLS_RSA_MIT_AES_128_GCM_SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 9D	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x9E	TLS_DHE_RSA_MIT_AES_128_GCM_SHA256	TLS_DHE_RSA_MIT_AES_128_GCM_SHA256	PFS + GPP PFS + Zertifikat
0 x 9F	TLS_DHE_RSA_MIT_AES_256_GCM_SHA384	TLS_DHE_RSA_MIT_AES_256_GCM_SHA384	PFS + GPP PFS + Zertifikat
0 x 1301	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	PFS + GPP PFS + Zertifikat
0 x 1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Zertifikat
0 x 1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Zertifikat
0xC007	TLS_ECDHE_ECDSA_MIT_RC4_SHA	TLS_ECDHE_ECDSA_MIT_RC4_SHA	PFS + GPP
0xC008	TLS_ECDHE_ECDSA_WITH_3DES_CBC_SHA	TLS_ECDHE_ECDSA_WITH_3DES_CBC_SHA	PFS + GPP
0xC009	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA	PFS + GPP
0xC011	TLS_ECDHE_RSA_MIT_RC4_SHA	TLS_ECDHE_RSA_MIT_RC4_SHA	PFS + GPP PFS + Zertifikat
0xC012	TLS_ECDHE_RSA_WITH_3DES_CBC_SHA	TLS_ECDHE_RSA_WITH_3DES_CBC_SHA	PFS + GPP PFS + Zertifikat
0xC013	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA	PFS + GPP PFS + Zertifikat
0xC014	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA	PFS + GPP PFS + Zertifikat
0xC023	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA256	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA256	PFS + GPP

Hex-Wert	Vorname (IANA)	Name (OpenSSL)	Unterstützte Entschlüsselung
0xC024	TLS_ECDHE_ECDSA_MIT_AE	CDHE_ECDSA_SHA256 ECDHE_ECDSA_SHA256	PFS + GPP
0xC027	TLS_ECDHE_RSA_MIT_AE	CDHE_RSA_SHA256 ECDHE_RSA_SHA256	PFS + GPP PFS + Zertifikat
0xC028	TLS_ECDHE_RSA_MIT_AE	CDHE_RSA_SHA384 ECDHE_RSA_SHA384	PFS + GPP PFS + Zertifikat
0xC02B	TLS_ECDHE_ECDSA_MIT_AE	CDHE_ECDSA_SHA256 ECDHE_ECDSA_SHA256	PFS + GPP
0xC02C	TLS_ECDHE_ECDSA_MIT_AE	CDHE_ECDSA_SHA384 ECDHE_ECDSA_SHA384	PFS + GPP
0xC02F	TLS_ECDHE_RSA_MIT_AE	CDHE_RSA_SHA256 ECDHE_RSA_SHA256	PFS + GPP PFS + Zertifikat
0xC030	TLS_ECDHE_RSA_MIT_AE	CDHE_RSA_SHA384 ECDHE_RSA_SHA384	PFS + GPP PFS + Zertifikat
0xCCA8	TLS_ECDHE_RSA_MIT_CHA	CDHE_RSA ECDHE_RSA	PFS + GPP PFS + Zertifikat
0xCCA9	TLS_ECDHE_ECDSA_MIT_CHA	CDHE_ECDSA ECDHE_ECDSA	PFS + GPP
0xCCAA	TLS_DHE_RSA_MIT_CHA	CDHE_RSA DHE_RSA	PFS + GPP PFS + Zertifikat