Suites de chiffrement SSL/TLS prises en charge

Publié: 2024-07-02

Le système ExtraHop peut déchiffrer le trafic SSL/TLS qui a été chiffré avec des suites de chiffrement PFS ou RSA. Toutes les suites de chiffrement prises en charge peuvent être déchiffrées en installant le redirecteur de clé de session sur un serveur et en configurant le système ExtraHop.

Les suites de chiffrement pour RSA peuvent également déchiffrer le trafic à l'aide d'un certificat et d'une clé privée, avec ou sans transfert de clé de session.

Méthodes de déchiffrement

Le tableau ci-dessous fournit une liste des suites de chiffrement que le système ExtraHop peut utiliser décrypter ainsi que les options de déchiffrement prises en charge.

- **PFS + GPP**: le système ExtraHop peut déchiffrer ces suites de chiffrement avec transfert de clé de session et mappage global entre protocole et port
- **Certificat PFS +**: le système ExtraHop peut déchiffrer ces suites de chiffrement avec le transfert de clé de session et le certificat et clé privée
- **Certificat RSA +**: le système ExtraHop peut déchiffrer ces suites de chiffrement sans transfert de clé de session tant que vous avez téléchargé le certificat et clé privée

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0x04	TLS_RSA_AVEC_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Certificat RSA + Certificat
0x05	TLS_RSA_AVEC_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Certificat
0x2F	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Certificat
0x35	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Certificat
0x3C	TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Certificat RSA + Certificat

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0x3D	TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Certificat
0 x 6B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Certificat
0x9C	TLS_RSA_AVEC_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x9D	TLS_RSA_AVEC_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Certificat RSA + Certificat
0 x 9	TLS_DHE_RSA_AVEC_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Certificat
0 x 9 F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Certificat
0x1301	TLS_AES_128_GCM_SHA255	TLS_AES_128_GCM_SHA255	PFS + GPP PFS + Certificat
0x1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Certificat
0x1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Certificat
0 x C007	TLS_ECDHE_ECDSA_AVEC_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS + GPP
0 x C008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS + GPP
0 x C009	TLS_ECDHE_ECDSA_AVEC_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP
0 x C011	TLS_ECDHE_RSA_AVEC_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Certificat
0 x C012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Certificat
0 x C013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Certificat
0 x C014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Certificat
0 x C023	TLS_ECDHE_ECDSA_AVEC_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0 x C024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0 x C027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Certificat
0 x C028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Certificat
0xC02B	TLS_ECDHE_ECDSA_AVEC_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP
0xC02C	TLS_ECDHE_ECDSA_AVEC_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP
0xC02F	TLS_ECDHE_RSA_AVEC_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Certificat
0 x C030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Certificat
0 x CCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Certificat
0 x CCA9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305	PFS + GPP
0 x CCAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Certificat