

Déchiffrez le trafic TLS à l'aide de certificats et de clés privées

Publié: 2024-11-03

Vous pouvez déchiffrer le trafic TLS transféré en téléchargeant la clé privée et le certificat de serveur associés à ce trafic. Le certificat et la clé sont téléchargés via une connexion HTTPS depuis un navigateur Web vers le système ExtraHop.

Après le téléchargement, les clés privées sont cryptées et stockées sur le système ExtraHop. Pour s'assurer que les clés privées ne sont pas transférables vers d'autres systèmes, elles sont cryptées à l'aide d'une clé interne contenant des informations spécifiques au système sur lequel elles ont été téléchargées.

La séparation des privilèges est appliquée afin que seul le processus de déchiffrement TLS du système puisse accéder aux clés privées. Vous pouvez ajouter de nouvelles clés privées via les paramètres d'administration, mais vous ne pouvez pas accéder aux clés privées stockées.



Note: Votre trafic doit être chiffré à l'aide d'un [suite de chiffrement prise en charge](#). En savoir plus sur [Décryptage TLS](#).

Téléchargez un certificat PEM et une clé privée RSA



Conseil Vous pouvez exporter une clé protégée par mot de passe à ajouter à votre système ExtraHop en exécutant la commande suivante sur un programme tel qu'OpenSSL :

```
openssl rsa -in yourcert.pem -out new.key
```

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décryptage SSL**.
4. Dans le Décryptage par clé privée section, cochez la case pour **Exiger des clés privées**.
5. Cliquez **Enregistrer**.
6. Dans le Clés privées section, cliquez sur **Ajouter des clés**.
7. Dans le Nom dans ce champ, saisissez un nom descriptif pour identifier ce certificat et cette clé.
8. Effacez le **Activé** case à cocher si vous souhaitez désactiver ce certificat TLS.
9. Dans le Certificat champ, collez le certificat de clé publique.
10. Dans le Clé privée dans le champ, collez la clé privée RSA.
11. Cliquez **Ajouter**.

Prochaines étapes

[Ajoutez les protocoles chiffrés](#) vous souhaitez déchiffrer avec ce certificat.

Téléchargez un fichier PKCS #12 /PFX

Les fichiers PKCS #12 /PFX sont archivés dans un conteneur sécurisé sur le système ExtraHop et contiennent des paires de clés publiques et privées, accessibles uniquement par mot de passe.



Conseil Pour exporter des clés privées d'un KeyStore Java vers un fichier PKCS #12, exécutez la commande suivante sur votre serveur, où `javakeystore.jks` est le chemin de votre KeyStore Java :

```
keytool -importkeystore -srckeystore javakeystore.jks -
destkeystore
pkcs.p12 -srcstoretype jks -deststoretype pkcs12
```

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décryptage SSL**.
4. Dans le Décryptage par clé privée section, cochez la case pour **Exiger des clés privées**.
5. Cliquez **Enregistrer**.
6. Dans le Clés privées section, cliquez sur **Ajouter des clés**.
7. Dans le Ajouter un fichier PKCS #12 / PFX avec mot de passe section, dans le champ Description, saisissez un nom descriptif pour identifier ce certificat et cette clé.
8. Effacez le **Activé** case à cocher si vous souhaitez désactiver ce certificat TLS.
9. Pour Fichier PKCS #12 / PFX, cliquez **Naviguez**.
10. Accédez au fichier et sélectionnez-le, puis cliquez sur **Ouvrir**.
11. Dans le Mot de passe dans le champ, saisissez le mot de passe du fichier PKCS #12 / PFX.
12. Cliquez **Ajouter**.
13. Cliquez **OK**.

Prochaines étapes

Ajoutez les protocoles chiffrés vous souhaitez déchiffrer à l'aide de ce certificat.

Ajouter des protocoles chiffrés

Vous devez ajouter chaque protocole que vous souhaitez déchiffrer pour chaque certificat téléchargé.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décryptage SSL**.
4. Dans le Mappage du protocole au port par clé section, cliquez sur **Ajouter un protocole**.
5. À partir du **Protocole** dans la liste déroulante, sélectionnez le protocole que vous souhaitez déchiffrer.
6. À partir du **Clé** dans la liste déroulante, sélectionnez une clé privée téléchargée.
7. Dans le Port dans le champ, saisissez le port source du protocole.
La valeur par défaut est 443, qui indique le trafic HTTP. Spécifiez 0 pour déchiffrer tout le trafic du protocole.
8. Cliquez **Ajouter**.

Suites de chiffrement TLS prises en charge

Le système ExtraHop peut déchiffrer le trafic TLS chiffré à l'aide de 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. [déchiffrer](#) 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 à l'aide du transfert de clé de session et du [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
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
0x6B	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

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
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_SHA256	TLS_AES_128_GCM_SHA256	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
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

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
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