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

Publié: 2024-02-21

Vous pouvez déchiffrer le trafic SSL 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 garantir que les clés privées ne sont pas transférables à d'autres systèmes, elles sont chiffrées 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 SSL du système puisse accéder aux clés privées. Bien que vous puissiez ajouter de nouvelles clés privées via les paramètres d' administration, vous ne pouvez pas accéder aux clés privées stockées.

Note: Votre trafic doit être crypté avec un suite de chiffrement prise en charge. En savoir plus sur Déchiffrement SSL/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 la section Configuration du système, cliquez sur **Capturez**.
3. Cliquez **Déchiffrement SSL**.
4. Dans le Déchiffrement par clé privée section, cochez la case pour **Exiger des clés privées**.
5. Cliquez **Enregistrer**.
6. Dans la section Clés privées, cliquez sur **Ajouter des clés**.
7. Dans le Ajouter un certificat PEM et une clé privée RSA section, entrez les informations suivantes :

   Nom

   Nom descriptif permettant d'identifier ce certificat et cette clé.

   Activé

   Décochez cette case si vous souhaitez désactiver ce certificat SSL.

   Certificat

   Le certificat de clé publique.

   Clé privée

   La clé privée RSA.
8. 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, entrez les informations suivantes :

   Descriptif

   Nom descriptif permettant d'identifier ce certificat et cette clé.

   Activé

   Décochez cette case pour désactiver ce certificat SSL.
8. À côté du fichier PKCS #12 /PFX, cliquez sur **Choisissez un fichier**.
9. Accédez au fichier et sélectionnez-le, puis cliquez sur **Ouvrir**.
10. Dans le champ Mot de passe, saisissez le mot de passe du fichier PKCS #12 /PFX.
11. Cliquez **Ajouter**.
12. Cliquez **OK.**.

Prochaines étapes
Ajoutez les protocoles chiffrés vous souhaitez déchiffrer avec 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 la section Configuration du système, cliquez sur **Capture**.
3. Cliquez **Déchiffrement SSL**.
4. Dans le Mappage du protocole au port par clé section, cliquez **Ajouter un protocole**.
5. Sur le Ajouter un protocole crypté page, entrez les informations suivantes :

   Protocole

   Dans la liste déroulante, sélectionnez le protocole que vous souhaitez déchiffrer.

   Clé

   Dans la liste déroulante, sélectionnez une clé privée téléchargée.

Port

Entrez le port source du protocole. Par défaut, cette valeur est définie sur 443, ce qui indique le trafic HTTP. Spécifiez 0 pour déchiffrer tout le trafic du protocole.

6. Cliquez **Ajouter**.

Suites de chiffrement SSL/TLS prises en charge

Le système ExtraHop peut déchiffrer le trafic SSL/TLS 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 décrypter ainsi que les options de déchiffrement prises en charge.

- **PFS+GPP**: le système ExtraHop peut déchiffrer ces suites de chiffrement grâce au transfert de clé de session et mappage global du protocole au port
- **Certificat PFS +**: le système ExtraHop peut déchiffrer ces suites de chiffrement grâce au transfert de clé de session et au 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)	Déchiffrement pris en charge
0x04	TLS_RSA_WITH_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Certificat RSA + Certificat
0x05	TLS_RSA_WITH_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
0 x 16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	Certificat PFS + GPP PFS +
0 x 2 F	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	Certificat PFS + GPP PFS +
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	Certificat PFS + GPP PFS +

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Déchiffrement pris en charge
0 x 3 C	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	Certificat PFS + GPP PFS +
0 x 6 B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	Certificat PFS + GPP PFS +
0 x 9C	TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0 x 9D	TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Certificat RSA + Certificat
0 x 9E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	Certificat PFS + GPP PFS +
0 x 9F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	Certificat PFS + GPP PFS +
0x1301	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	Certificat PFS + GPP PFS +
0x1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	Certificat PFS + GPP PFS +
0x1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	Certificat PFS + GPP PFS +
0xC007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS+GPP
0xC008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS+GPP
0xC009	TLS_ECDHE_ECDSA_WITH_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_WITH_RC4_128_SHA	ECDHE-RSA-RC4-SHA	Certificat PFS + GPP PFS +
0 x C012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	Certificat PFS + GPP PFS +
0 x C013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	Certificat PFS + GPP PFS +
0 x C014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	Certificat PFS + GPP PFS +

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Déchiffrement pris en charge
0xC023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS+GPP
0xC024	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	Certificat PFS + GPP PFS +
0 x C028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	Certificat PFS + GPP PFS +
0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS+GPP
0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS+GPP
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	Certificat PFS + GPP PFS +
0xC030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	Certificat PFS + GPP PFS +
0 x CCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	Certificat PFS + GPP PFS +
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	Certificat PFS + GPP PFS +