Entschlüsseln Sie den SSL-Verkehr mit Zertifikaten und privaten Schlüsseln

Veröffentlicht: 2024-02-12

Sie können weitergeleiteten SSL-Verkehr entschlüsseln, indem Sie den privaten Schlüssel und das Serverzertifikat hochladen, die diesem Verkehr zugeordnet sind. Das Zertifikat und der Schlüssel werden über eine HTTPS-Verbindung von einem Webbrowser in das ExtraHop-System hochgeladen.

Nach dem Upload werden private Schlüssel verschlüsselt und auf dem ExtraHop-System gespeichert. Um sicherzustellen , dass private Schlüssel nicht auf andere Systeme übertragbar sind, werden sie mit einem internen Schlüssel verschlüsselt, der spezifische Informationen für das System enthält, auf das sie hochgeladen wurden.

Die Trennung der Rechte wird erzwungen, sodass nur der SSL-Entschlüsselungsprozess auf dem System auf die privaten Schlüssel zugreifen kann. Sie können zwar über die Administrationseinstellungen neue private Schlüssel hinzufügen, aber Sie können nicht auf gespeicherte private Schlüssel zugreifen.

Hinweis: Ihr Datenverkehr muss verschlüsselt sein mit einem unterstützte Verschlüsselungssuite. Erfahre mehr über SSL/TLS-Entschlüsselung.

Laden Sie ein PEM-Zertifikat und einen privaten RSA-Schlüssel hoch

Hinweis: Sie können einen kennwortgeschützten Schlüssel exportieren, um ihn Ihrem ExtraHop-System hinzuzufügen, indem Sie den folgenden Befehl in einem Programm wie OpenSSL ausführen:

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

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Systemkonfiguration auf **Erfassen**.
3. klicken **SSL-Entschlüsselung**.
4. In der Entschlüsselung von privaten Schlüsseln Abschnitt, aktivieren Sie das Kontrollkästchen für **Private Schlüssel erforderlich**.
5. klicken **Speichern**.
6. Klicken Sie im Abschnitt Private Keys auf **Schlüssel hinzufügen**.
7. In der PEM-Zertifikat und privaten RSA-Schlüssel hinzufügen Abschnitt, geben Sie die folgenden Informationen ein:

   Name
   Ein beschreibender Name zur Identifizierung dieses Zertifikats und Schlüssels.

   Aktiviert
   Deaktivieren Sie dieses Kontrollkästchen, wenn Sie dieses SSL-Zertifikat deaktivieren möchten.

   Zertifikat
   Das Public-Key-Zertifikat.

   Privater Schlüssel
   Der private RSA-Schlüssel.
8. klicken **Hinzufügen**.

Nächste Schritte
Fügen Sie die verschlüsselten Protokolle hinzu Sie möchten mit diesem Zertifikat entschlüsseln.

Laden Sie eine PKCS #12 /PFX-Datei hoch

PKCS #12 /PFX-Dateien werden in einem sicheren Container auf dem ExtraHop-System archiviert und enthalten sowohl öffentliche als auch private Schlüsselpaare, auf die nur mit einem Passwort zugegriffen werden kann.

Hinweis: Um private Schlüssel aus einem Java KeyStore in eine PKCS #12 -Datei zu exportieren, führen Sie den folgenden Befehl auf Ihrem Server aus, wobei `javakeystore.jks` ist der Pfad Ihres Java-KeyStores:

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

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. Klicken Sie **SSL-Entschlüsselung**.
4. In der Entschlüsselung des privaten Schlüssels Abschnitt, wählen Sie das Kontrollkästchen für **Private Schlüssel erforderlich**.
5. Klicken Sie **Speichern**.
6. In der Private Schlüssel Abschnitt, klicken **Schlüssel hinzufügen**.
7. In der PKCS #12 /PFX-Datei mit Passwort hinzufügen Abschnitt, geben Sie die folgenden Informationen ein:

   Beschreibung

   Ein beschreibender Name zur Identifizierung dieses Zertifikats und Schlüssels.

   Aktiviert

   Deaktivieren Sie dieses Kontrollkästchen, um dieses SSL-Zertifikat zu deaktivieren.
8. Klicken Sie neben der Datei PKCS #12 /PFX auf **Wählen Sie Datei**.
9. Navigieren Sie zu der Datei, wählen Sie sie aus und klicken Sie dann auf **Offen**.
10. Geben Sie im Feld Passwort das Passwort für die PKCS #12 /PFX-Datei ein.
11. Klicken Sie **Hinzufügen**.
12. Klicken Sie **OK**.

Nächste Schritte

Fügen Sie die verschlüsselten Protokolle hinzu Sie möchten mit diesem Zertifikat entschlüsseln.

Verschlüsselte Protokolle hinzufügen

Sie müssen jedes Protokoll, das Sie entschlüsseln möchten, für jedes hochgeladene Zertifikat hinzufügen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Systemkonfiguration auf **Erfassen**.
3. klicken **SSL-Entschlüsselung**.
4. In der Zuordnung von Protokoll zu Port nach Schlüssel Abschnitt, klicken **Protokoll hinzufügen**.
5. Auf dem Verschlüsseltes Protokoll hinzufügen Seite, geben Sie die folgenden Informationen ein:

   Protokoll

   Wählen Sie aus der Dropdownliste das Protokoll aus, das Sie entschlüsseln möchten.

Schlüssel

Wählen Sie aus der Drop-down-Liste einen hochgeladenen privaten Schlüssel aus.

Hafen

Geben Sie den Quellport für das Protokoll ein. Standardmäßig ist dieser Wert auf 443 gesetzt, was den HTTP-Verkehr angibt. Geben Sie 0 an, um den gesamten Protokollverkehr zu entschlüsseln.

6. klicken **Hinzufügen**.

Unterstützte SSL/TLS-Verschlüsselungssammlungen

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	RC4-MD5	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 05	TLS_RSA_MIT_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0x2F	TLS_RSA_MIT_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 33	TLS_DHE_RSA_MIT_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0 x 35	TLS_RSA_MIT_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat

Hex-Wert	Vorname (IANA)	Name (OpenSSL)	Unterstützte Entschlüsselung
0 x 39	TLS_DHE_RSA_MIT_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0x3C	TLS_RSA_MIT_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x3D	TLS_RSA_MIT_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 67	TLS_DHE_RSA_MIT_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0 x 6 B	TLS_DHE_RSA_MIT_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Zertifikat
0 x 9 C	TLS_RSA_MIT_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 9D	TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x9E	TLS_DHE_RSA_MIT_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0 x 9F	TLS_DHE_RSA_MIT_AES_256_GCM_SHA384	DHE-RSA-AES256-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_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_MIT_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP
0xC011	TLS_ECDHE_RSA_MIT_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Zertifikat
0xC012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0xC013	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat

Hex-Wert	Vorname (IANA)	Name (OpenSSL)	Unterstützte Entschlüsselung
0xC014	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0xC023	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP
0xC024	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0xC027	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0xC028	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Zertifikat
0xC02B	TLS_ECDHE_ECDSA_MIT_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP
0xC02C	TLS_ECDHE_ECDSA_MIT_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP
0xC02F	TLS_ECDHE_RSA_MIT_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0xC030	TLS_ECDHE_RSA_MIT_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat
0xCCA8	TLS_ECDHE_RSA_MIT_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat
0xCCA9	TLS_ECDHE_ECDSA_MIT_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305	PFS + GPP
0xCCAA	TLS_DHE_RSA_MIT_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat