# Installieren Sie den ExtraHop Session Key Forwarder auf einem Linux-Server

Veröffentlicht: 2023-12-05

Perfect Forward Secrecy (PFS) ist eine Eigenschaft sicherer Kommunikationsprotokolle, die einen kurzfristigen, vollständig privaten Sitzungsschlüsselaustausch zwischen Clients und Servern ermöglicht. ExtraHop bietet eine Software zur Weiterleitung von Sitzungsschlüsseln, die Sitzungsschlüssel zur SSL/TLS-Entschlüsselung an das ExtraHop-System senden kann. Kommunikation zwischen dem Schlüsselspediteur und dem Sensor ist mit TLS 1.2 oder TLS 1.3 verschlüsselt, und die Anzahl der Sitzungsschlüssel, die das ExtraHop-System empfangen kann, ist unbegrenzt.

Sie müssen das ExtraHop-System für die Weiterleitung von Sitzungsschlüsseln konfigurieren und dann die Forwarder-Software auf dem installieren Fenster und Linux Server mit dem SSL/TLS-Verkehr , den Sie entschlüsseln möchten.

Bevor du anfängst

- Lesen Sie über SSL/TLS-Entschlüsselung und überprüfen Sie die Liste von unterstützte Cipher Suites.
- Stellen Sie sicher, dass das ExtraHop-System für SSL Decryption und SSL Shared Secrets lizenziert ist.
- Stellen Sie sicher, dass Ihre Serverumgebung von der ExtraHop-Sitzungsschlüsselweiterleitungssoftware unterstützt wird:
  - Microsoft Secure Channel (Schannel) -Sicherheitspaket
  - Java SSL/TLS (Java-Versionen 8 bis 13). Führen Sie kein Upgrade auf diese Version der Sitzungsschlüsselweiterleitung durch, wenn Sie derzeit Java 6- oder Java 7-Umgebungen überwachen. Version 7.9 des Session Key Forwarders unterstützt Java 6 und Java 7 und ist mit der neuesten ExtraHop-Firmware kompatibel.
  - Dynamisch verknüpfte OpenSSL-Bibliotheken (1.0.x und 1.1.x). OpenSSL wird nur auf Linux-Systemen mit Kernelversionen 4.4 und höher und RHEL 7.6 und höher unterstützt.
- Stellen Sie sicher, dass der Server, auf dem Sie den Session Key Forwarder installieren, dem SSL-Zertifikat des ExtraHop vertraut. Sensor.
- Stellen Sie sicher, dass Ihre Firewallregeln zulassen, dass vom überwachten Server Verbindungen zum TCP-Port 4873 auf dem Sensor initiiert werden.

  **Wichtig:** Das ExtraHop-System kann den TLS-verschlüsselten TDS-Verkehr nicht über die Weiterleitung von Sitzungsschlüsseln entschlüsseln. Stattdessen können Sie eine RSA hochladen privater Schlüssel.

- Installieren Sie den Session Key Forwarder auf RHEL-, CentOS-, Fedora- oder Debian-Ubuntu-Linux-Distributionen. Die Sitzungsschlüsselweiterleitung funktioniert auf anderen Distributionen möglicherweise nicht richtig.
- Der Session Key Forwarder wurde nicht ausführlich mit SELinux getestet und ist möglicherweise nicht kompatibel, wenn er auf einigen Linux-Distributionen aktiviert ist.

## Aktivieren Sie den SSL-Sitzungsschlüsselempfängerdienst

Sie müssen den Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktivieren, bevor das System Sitzungsschlüssel vom Sitzungsschlüsselweiterleiter empfangen und entschlüsseln kann. Standardmäßig ist dieser Dienst deaktiviert.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Appliance-Einstellungen auf **Dienstleistungen**.
3. Wählen Sie den **SSL-Sitzungsschlüsselempfänger** Checkbox.

4. klicken **Speichern**.

## Einen globalen Port zur Protokollzuordnung hinzufügen

Fügen Sie jedes Protokoll für den Datenverkehr hinzu, den Sie mit Ihren Sitzungsschlüsselweiterleitungen entschlüsseln möchten.

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. Löschen Sie im Abschnitt Private Key Decryption den Private Schlüssel erforderlich Checkbox.
5. Klicken Sie im Abschnitt Global Protocol to Port Mapping auf **Globales Protokoll hinzufügen**.
6. Wählen Sie in der Dropdownliste Protokoll das Protokoll für den Datenverkehr aus, den Sie entschlüsseln möchten.
7. Geben Sie im Feld Port die Nummer des Ports ein. Typ `0` um alle Ports hinzuzufügen.
8. klicken **Hinzufügen**.

## Installieren Sie die Software

### RPM-basierte Distributionen

**Hinweis:** Sie können den Forwarder ohne Benutzerinteraktion installieren, indem Sie spezifizieren Umgebungsvariablen im Installationsbefehl.

1. Melden Sie sich bei Ihrem RPM-basierten Linux-Server an.
2. Herunterladen die neueste Version des ExtraHop-Sitzungsschlüsselweiterleitungssoftware.
3. Öffnen Sie eine Terminal-Anwendung und führen Sie den folgenden Befehl aus:

```
sudo rpm --install <path to installer file>
```

4. Öffnen Sie das Initialisierungsskript in einem Texteditor (vi oder vim, für Beispiel).

```
sudo vi /opt/extrahop/etc/extrahop-key-forwarder.conf
```

5. Je nachdem, wie dein Sensoren verwaltet werden, wählen Sie eine der folgenden Optionen Optionen:
   - Entfernen Sie bei selbstverwalteten Sensoren das Hashsymbol (#) vor dem EDA_HOSTNAME Feld und geben Sie den vollqualifizierten Domänenname Ihres Sensor ein, ähnlich wie folgendes Beispiel.

     ```
     EDA_HOSTNAME=discover.example.com
     ```

     **Hinweis:** Sie können Sitzungsschlüssel an mehr als einen Sensor weiterleiten, indem Sie Eingabe von kommagetrennten Hostnamen. Für Beispiel:

     ```
     EDA_HOSTNAME=packet-sensor.example.com,ids-sensor.example.com
     ```

   - Bei Sensoren mit Extrahop-Verwaltung entfernen Sie das Hashsymbol (#) vor dem `EDA_HOSTED_PLATFORM` Feld und Typ `aws`, ähnlich dem folgenden Beispiel.

     ```
     EDA_HOSTED_PLATFORM=aws
     ```

6. Optional: Der Key-Forwarder empfängt Sitzungsschlüssel lokal aus der Java-Umgebung über einen TCP-Listener auf localhost (127.0.0.1) und den Port, der in angegeben ist die `LOCAL_LISTENER_PORT` Feld. Wir haben empfohlen, dass Port bleibt auf der Standardeinstellung 598 gesetzt. Wenn Sie die Portnummer ändern, muss das ändern `-javaagent` Argument, um das Neue zu berücksichtigen Hafen.
7. Optional: Wenn Sie es vorziehen, dass Syslog in eine andere Einrichtung schreibt als `local3` für Key-Forwarder-Log-Meldungen können Sie das bearbeiten `SYSLOG` Feld.
   Bei einem selbstverwalteten Sensor ist der Inhalt des `extrahop-key-forwarder.conf` Datei sollte erscheinen ähnlich dem folgenden Beispiel:

   ```
   #EDA_HOSTED_PLATFORM=aws
   EDA_HOSTNAME=sensor.example.com
   LOCAL_LISTENER_PORT=598
   SYSLOG=local3
   ADDITIONAL_ARGS=''
   ```
8. Speichern Sie die Datei und beenden Sie den Texteditor.
9. Wenn Ihr Server Container mit der containerd-Laufzeit verwaltet, müssen Sie hinzufügen die folgenden Parameter für `/opt/extrahop/etc/extrahop-key-forwarder.conf` Aufbau datei:

   - `-containerd-enable`
   - `-containerd-socket`
   - `-containerd-state`
   - `-containerd-state-rootfs-subdir`

   Weitere Informationen zu diesen Parametern und anderen optionalen Parametern finden Sie sehen Optionen für die Weiterleitung von Sitzungsschlüsseln.
10. Starte das `extrahop-key-forwarder` Dienst:

    ```
    sudo service extrahop-key-forwarder start
    ```

## Debian-Ubuntu-Distributionen

**Hinweis:** Sie können den Forwarder ohne Benutzerinteraktion installieren, indem Sie spezifizieren Umgebungsvariablen im Installationsbefehl.

1. Melden Sie sich bei Ihrem Debian- oder Ubuntu-Linux-Server an.
2. Herunterladen die neueste Version des ExtraHop-Sitzungsschlüsselweiterleitungssoftware.
3. Öffnen Sie eine Terminalanwendung und führen Sie den folgenden Befehl aus.

   ```
   sudo dpkg --install <path to installer file>
   ```
4. Je nachdem, wie dein Sensoren verwaltet werden, wählen Sie eine der folgenden Optionen Optionen:

   - 1. Für Selbstverwaltete Sensoren, wählen **richten** und drücken Sie dann die EINGABETASTE.
     2. Geben Sie den vollqualifizierten Domänenname oder die IP-Adresse des ExtraHop-Systems ein, wobei Die Sitzungsschlüssel werden weitergeleitet und drücken Sie dann die EINGABETASTE.

        **Hinweis:** Sie können Sitzungsschlüssel an mehrere Sensor weiterleiten, indem Sie Folgendes eingeben kommagetrennte Hostnamen. Für Beispiel:

        ```
        packet-sensor.example.com,ids-sensor.example.com
        ```
   - Wählen Sie für von ExtraHop verwaltete Sensoren **gehostet** und drücken Sie dann die EINGABETASTE.
5. Wenn Ihr Server Container mit der containerd-Laufzeit verwaltet, müssen Sie hinzufügen die folgenden Parameter für `/opt/extrahop/etc/extrahop-key-forwarder.conf` Aufbau datei:

- `-containerd-enable`
- `-containerd-socket`
- `-containerd-state`
- `-containerd-state-rootfs-subdir`

Weitere Informationen zu diesen Parametern und anderen optionalen Parametern finden Sie sehen Optionen für die Weiterleitung von Sitzungsschlüsseln.

6. Stellen Sie sicher, dass der `extrahop-key-forwarder` Bedienung gestartet:

```
sudo service extrahop-key-forwarder status
```

Die folgende Ausgabe sollte erscheinen:

```
extrahop-key-forwarder.service - LSB: ExtraHop Session Key Forwarder
Loaded: loaded (/etc/rc.d/init.d/extrahop-key-forwarder; bad; vendor
 preset: disabled)
Active: active (running) since Tue 2018-04-10 10:55:47 PDT; 5s ago
```

Wenn der Dienst nicht aktiv ist, führen Sie Folgendes aus Befehl:

```
sudo service extrahop-key-forwarder start
```

### Integrieren Sie den Forwarder in die Java-basierte SSL-Anwendung

Der ExtraHop Session Key Forwarder lässt sich wie folgt in Java-Anwendungen integrieren die `-javaagent` Option. Konsultieren Sie die spezifischen Anforderungen Ihrer Anwendung Anweisungen zum Ändern der Java-Laufzeitumgebung, um `-javaagent` Option.

Als Beispiel viele Tomcat-Umgebungen unterstützt die Anpassung von Java-Optionen in der `/etc/default/tomcat7` Datei. Im folgenden Beispiel Hinzufügen der `-javaagent` Die Option zur JAVA_OPTS-Zeile bewirkt das Java-Laufzeit, um SSL-Sitzungsgeheimnisse mit dem Schlüsselweiterleitungsprozess zu teilen, die leitet dann die Geheimnisse an das ExtraHop-System weiter, damit die Geheimnisse entschlüsselt.

```
JAVA_OPTS="... -javaagent:/opt/extrahop/lib/exagent.jar
```

## Überprüfen Sie Ihre Installation und beheben Sie Fehler

Wenn Ihr Linux-Server Netzwerkzugriff auf das ExtraHop-System hat und die Server-SSL-Konfiguration dem Zertifikat des ExtraHop-Systems vertraut, das Sie bei der Installation des Session-Key-Forwarders angegeben haben, ist die Konfiguration abgeschlossen.

In Fällen, in denen Sie Probleme mit der Konfiguration haben könnten, enthält die Binärdatei für die Sitzungsschlüsselweiterleitung einen Testmodus, auf den Sie über die Befehlszeile zugreifen können, um Ihre Konfiguration zu testen .

1. Loggen Sie sich auf Ihrem Linux-Server ein.
2. Um Ihre Installation zu überprüfen, führen Sie einen ersten Test durch, indem Sie den folgenden Befehl ausführen:

```
/opt/extrahop/sbin/extrahop-agent -t=true -server <eda hostname>
```

Die folgende Ausgabe sollte erscheinen:

```
<timestamp> Performing connectivity test
<timestamp> No connectivity issues detected
```

Wenn es ein Konfigurationsproblem gibt, werden in der Ausgabe Tipps zur Fehlerbehebung angezeigt, die Ihnen helfen , das Problem zu beheben. Folgen Sie den Vorschlägen, um das Problem zu beheben, und führen Sie den Test dann erneut aus.

3. Sie können optional die Überschreibung des Zertifikatspfads und des Servernamens testen, indem Sie dem obigen Befehl die folgenden Optionen hinzufügen.
   - Geben Sie diese Option an, um das Zertifikat zu testen, ohne es dem Zertifikatsspeicher hinzuzufügen.

     ```
     -cert <file path to certificate>
     ```
   - Geben Sie diese Option an, um die Verbindung zu testen, falls eine Diskrepanz zwischen dem Hostnamen des ExtraHop-Systems, den der Forwarder kennt (SERVER), und dem allgemeinen Namen (CN), der im SSL-Zertifikat des ExtraHop-Systems angegeben ist, besteht.

     ```
     -server-name-override <common name>
     ```

### (Optional) Konfigurieren Sie eine Servernamenüberschreibung

Wenn zwischen dem Hostnamen des ExtraHop-Systems, den der Forwarder kennt (SERVER), und dem Common Name (CN), der im SSL-Zertifikat des ExtraHop-Systems angegeben ist, eine Diskrepanz besteht, muss der Forwarder mit der richtigen CN konfiguriert werden.

Es wird empfohlen, das selbstsignierte SSL-Zertifikat auf der Grundlage des Hostnamens aus dem Abschnitt SSL-Zertifikat der Administrationseinstellungen neu zu generieren, anstatt diesen Parameter anzugeben.

1. Loggen Sie sich auf Ihrem Linux-Server ein.
2. Öffnen Sie die Konfigurationsdatei in einem Texteditor.

   ```
   vi /opt/extrahop/etc/extrahop-key-forwarder.conf
   ```
3. Füge ein `SERVER_NAME_OVERRIDE` Parameter mit einem Wert des Namens, der im ExtraHop-System-SSL-Zertifikat gefunden wurde, ähnlich dem folgenden Beispiel:

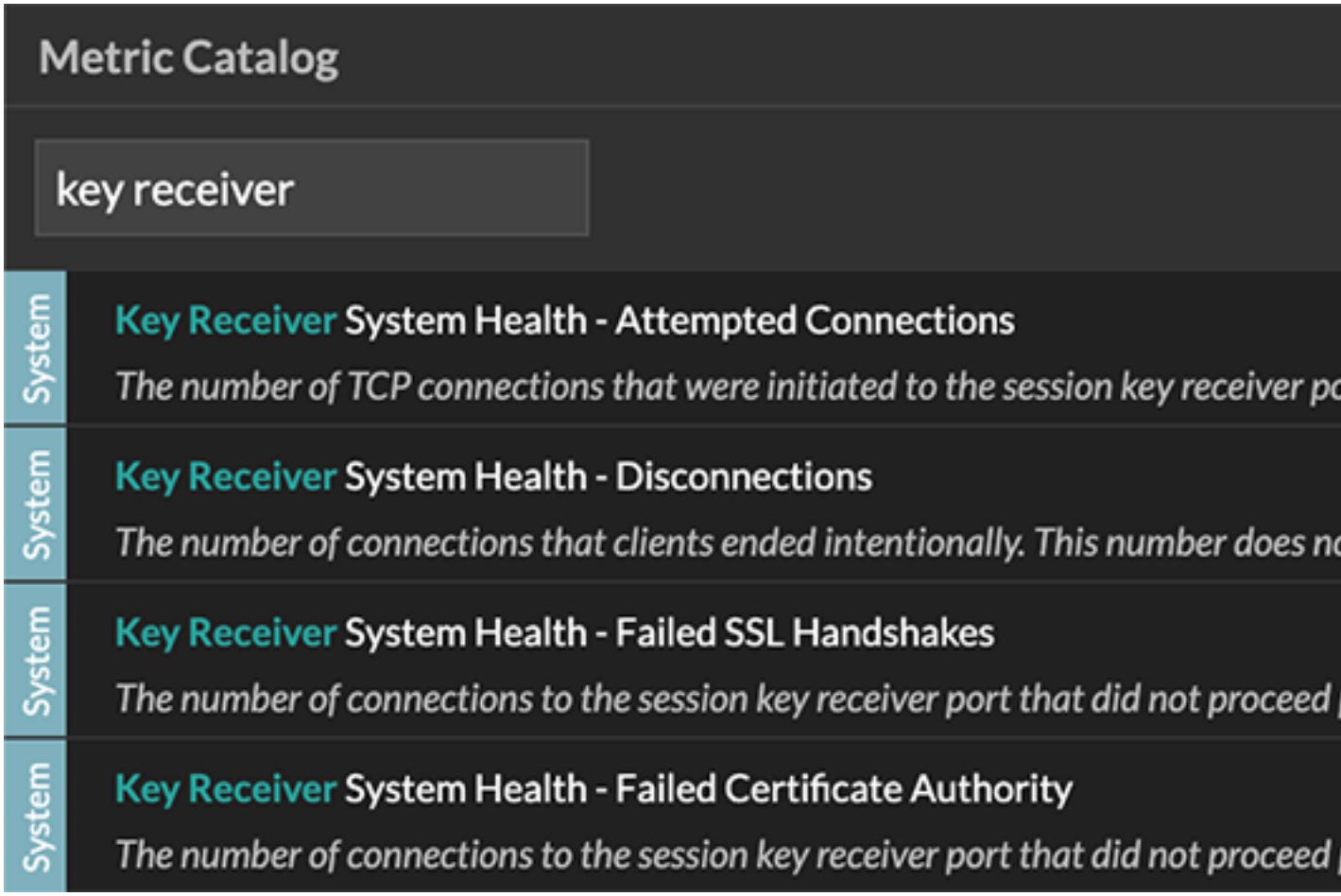
   ```
   SERVER_NAME_OVERRIDE=altname.example.com
   ```
4. Speichern Sie die Datei und beenden Sie den Texteditor.
5. Starte den `extrahop-key-forwarder` Bedienung.

   ```
   sudo service extrahop-key-forwarder start
   ```

## Wichtige Kennzahlen zum Zustand des Empfängersystems

Das ExtraHop-System bietet wichtige Empfängermetriken, die Sie zu einem Dashboard-Diagramm hinzufügen können, um den Zustand und die Funktionalität der wichtigsten Empfänger zu überwachen.

Um eine Liste der verfügbaren Messwerte anzuzeigen, klicken Sie auf das Symbol Systemeinstellungen ⚙ und dann klicken **Metrischer Katalog**. Typ `Schlüsselempfänger` im Filterfeld, um alle verfügbaren wichtigen Empfängermetriken anzuzeigen.




**Hinweis:** Informationen zum Erstellen eines neuen Dashboard-Diagramms finden Sie unter Bearbeiten Sie ein Diagramm mit dem Metric Explorer.

## Schlüsselweiterleitungen für verbundene Sitzungen anzeigen

Sie können kürzlich verbundene Sitzungsschlüsselweiterleitungen anzeigen, nachdem Sie die Sitzungsschlüsselweiterleitung auf Ihrem Server installiert und den SSL-Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktiviert haben. Beachten Sie, dass auf dieser Seite nur Sitzungsschlüsselweiterleitungen angezeigt werden, die in den letzten Minuten eine Verbindung hergestellt haben, nicht alle Sitzungsschlüsselweiterleitungen, die derzeit verbunden sind.

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 **Geteilte SSL-Geheimnisse**.

## Deinstalliere die Software

Wenn Sie die ExtraHop Session Key Forwarder-Software nicht mehr installieren möchten, führen Sie die folgenden Schritte aus.

1. Melden Sie sich beim Linux-Server an.
2. Öffnen Sie eine Terminalanwendung und wählen Sie eine der folgenden Optionen, um die Software zu entfernen.

- Führen Sie für RPM-basierte Server den folgenden Befehl aus:

  ```
  sudo rpm --erase extrahop-key-forwarder
  ```

- Führen Sie für Debian- und Ubuntu-Server den folgenden Befehl aus:

  ```
  sudo apt-get --purge remove extrahop-key-forwarder
  ```

  Typ `Y` wenn Sie aufgefordert werden, das Entfernen der Software zu bestätigen, und drücken Sie dann die EINGABETASTE.

3. klicken **Ja** zur Bestätigung.
4. Nachdem die Software entfernt wurde, klicken Sie auf **Ja** um das System neu zu starten

## Allgemeine Fehlermeldungen

Von der Sitzungsschlüsselweiterleitung verursachte Fehler werden in der Linux-Systemprotokolldatei protokolliert.

| Nachricht | Ursache | Lösung |
|---|---|---|
| `connect: dial tcp <IP address>:4873: connectex: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond` | Der überwachte Server kann keinen Verkehr an den weiterleiten Sensor. | Stellen Sie sicher, dass die Firewallregeln die Initiierung von Verbindungen durch den überwachten Server zum TCP-Port 4873 auf dem Sensor. |
| `connect: dial tcp <IP address>:4873: connectex: No connection could be made because the target machine actively refused it` | Der überwachte Server kann den Verkehr weiterleiten an Sensor, aber der Empfangsprozess hört nicht zu. | Stellen Sie sicher, dass Sensor ist sowohl für die Funktionen SSL Decryption als auch SSL Shared Secrets lizenziert. |
| `connect: x509: certificate signed by unknown authority` | Der überwachte Server kann das nicht verketten Sensor Zertifikat für eine vertrauenswürdige Zertifizierungsstelle (CA). | Stellen Sie sicher, dass der Linux-Zertifikatsspeicher für das Computerkonto über vertrauenswürdige Stammzertifizierungsstellen verfügt, die eine Vertrauenskette für das Sensor. |
| `connect: x509: cannot validate certificate for <IP address> because it doesn't contain any IP SANs` | Eine IP-Adresse wurde bereitgestellt als `SERVER` Parameter bei der Installation des Forwarders, aber das vom Sensor vorgelegte SSL-Zertifikat enthält keine IP-Adresse als Subject Alternate Name (SAN). | Wählen Sie aus den folgenden drei Lösungen.<br>• Ersetzen Sie die IP-Adresse für `SERVER` Wert in der `/etc/init.d/extrahop-key-forwarder` Datei mit einem Hostnamen. Der Hostname muss mit dem Betreffnamen |

| Nachricht | Ursache | Lösung |
|---|---|---|
| | | im Sensorzertifikat übereinstimmen. |
| | | • Wenn der Server eine Verbindung mit dem herstellen muss Sensor nach IP-Adresse, deinstallieren Sie den Forwarder und installieren Sie ihn erneut, wobei Sie den Betreffnamen aus dem Sensorzertifikat als Wert von angeben `server-name-override`. |
| | | • Neuausgabe der Sensor Zertifikat, das einen IP Subject Alternative Name (SAN) für die angegebene IP-Adresse enthält. |

## 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 |

| Hex-Wert | Vorname (IANA) | Name (OpenSSL) | Unterstützte Entschlüsselung |
|---|---|---|---|
| 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 |
| 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 |

| Hex-Wert | Vorname (IANA) | Name (OpenSSL) | Unterstützte Entschlüsselung |
|---|---|---|---|
| 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 |
| 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 |

## Optionen für die Weiterleitung von Sitzungsschlüsseln

Sie können die Sitzungsschlüsselweiterleitung konfigurieren, indem Sie das bearbeiten `/opt/extrahop/etc/extrahop-key-forwarder.conf` Datei.

In der folgenden Tabelle sind alle konfigurierbaren Optionen aufgeführt.

**Wichtig:** Wenn Sie Optionen hinzufügen `extrahop-key-forwarder.conf` die keine dedizierten Variablen haben, sie muss in der `ADDITIONAL_ARGS` Feld. Für Beispiel:

```
ADDITIONAL_ARGS="-v=true -libcrypto=/some/path/libcrypto.so
-libcrypto=/some/other/path/libcrypto.so"
```

| Option | Beschreibung |
|---|---|
| `-cert <path>` | Gibt den Pfad zum Serverzertifikat an. Geben Sie nur das an Option, wenn das Serverzertifikat nicht von einem vertrauenswürdigen Zertifikat signiert ist Autorität. |
| `-containerd-enable` | Aktiviert die Aufzählung von Containern, die mit der containerd-Laufzeit verwaltet werden. Das Die Option ist standardmäßig deaktiviert. Du musst tippen `-containerd-enable` zu aktiviere Container-Unterstützung. |
| `-containerd-socket <string>` | Der vollständige Pfad der containerd-Socket-Datei. |
| `-containerd-state <string>` | Der vollständige Pfad des containerd-State-Verzeichnisses. |
| `-containerd-state-rootfs-subdir <string>` | Der relative Pfad des `rootfs` Unterverzeichnis des Containerd Bundesstaatenverzeichnis. |
| `-docker-enable` | Aktiviert die Aufzählung von Docker-Containern. Diese Option wird aktiviert durch Standard. Du musst tippen `-docker-enable=falsch` um Docker zu deaktivieren Unterstützung. |
| `-docker-envoy <path>` | Gibt zusätzliche Envoy-Pfade innerhalb von Docker-Containern an. Sie können dies angeben Option mehrfach. |
| `-docker-go-binary <value>` | Gibt Glob-Muster an, um Go-Binärdateien in Docker-Containern zu finden. Du kannst geben Sie diese Option mehrmals an. |
| `-docker-libcrypto <path>` | Gibt den Pfad zu libcrypto innerhalb von Docker-Containern an. Sie können dies angeben Option mehrfach. |
| `-envoy <path>` | Gibt zusätzliche Envoy-Pfade auf dem Host an. Sie können diese Option angeben mehrfach. |
| `-go-binary <value>` | Gibt Glob-Muster an, um Go-Binärdateien zu finden. Sie können diese Option angeben mehrfach. |
| `-hearbeat-interval` | Gibt das Zeitintervall in Sekunden zwischen Heartbeat-Meldungen an. Das Standardintervall ist 30 Sekunden. |
| `-host-mount-path <path>` | Gibt den Pfad an, in den das Host-Dateisystem gemountet wird, wenn das ausgeführt wird Sitzungsschlüsselweiterleitung innerhalb eines Containers. |
| `-hosted <platform>` | Gibt an, dass der Agent auf der angegebenen gehosteten Plattform ausgeführt wird. Das Die Plattform ist derzeit beschränkt auf `aws`. |

| Option | Beschreibung |
|---|---|
| `-ldconfig-cache <path>` | Gibt den Pfad zum ldconfig-Cache an, ld.so.cache. Der Standardpfad ist `/etc/ld.so.cache`. Sie können diese Option mehrfach angeben mal. |
| `-libcrypto <path>` | Gibt den Pfad zur OpenSSL-Bibliothek an, `libcrypto`. Sie können diese Option mehrmals angeben, wenn Sie mehrere Installationen von OpenSSL. |
| `-no-docker-envoy` | Deaktiviert die Envoy-Unterstützung in Docker-Containern. |
| `-no-envoy` | Deaktiviert die Envoy-Unterstützung auf dem Host. |
| `-openssl-discover` | Erkennt automatisch `libcrypto` Implementierungen. Der Standardwert ist „true“. Du musst tippen `-openssl-discover=falsch` um OpenSSL zu deaktivieren Entschlüsselung. |
| `-pidfile <path>` | Gibt die Datei an, in der dieser Server seine Prozess-ID aufzeichnet. (PID). |
| `-port <value>` | Gibt den TCP-Port an, den der Sensor wartet auf Forward Sitzungsschlüssel. Der Standardport ist 4873. |
| `-server <string>` | Gibt den vollqualifizierten Domänenname des ExtraHop Discover an Gerät. |
| `-server-name-override <value>` | Gibt den Betreffnamen aus dem Sensor Zertifikat. Spezifizieren Sie dies Option, wenn dieser Server nur eine Verbindung zum Paket herstellen kann Sensor nach IP-Adresse. |
| `-syslog <facility>` | Gibt die Einrichtung an, die von der Schlüsselweiterleitung gesendet wurde. Die Standardeinstellung Einrichtung ist local3. |
| `-t` | Führen Sie einen Konnektivitätstest durch. Du musst tippen `-t=wahr` zu mit dieser Option ausführen. |
| `-tcp-listen-port <value>` | Gibt den TCP-Port an, auf den die Schlüsselweiterleitung wartet weitergeleitete Sitzungsschlüssel. |
| `-username <string>` | Gibt den Benutzer an, unter dem die Sitzungsschlüsselweiterleitung ausgeführt wird Die Forwarder-Software ist installiert. |
| `-v` | Aktivieren Sie die ausführliche Protokollierung. Du musst tippen `-v=true` rennen mit dieser Option. |

**Linux-Umgebungsvariablen**

Mit den folgenden Umgebungsvariablen können Sie die Sitzungsschlüsselweiterleitung installieren, ohne Benutzerinteraktion.

| Variabel | Beschreibung | Beispiel |
|---|---|---|
| `EXTRAHOP_CONNECTION_MODE` | Gibt den Verbindungsmodus zum Sitzungsschlüsselempfänger an. Die Optionen sind `richten` für selbstverwaltete Sensoren und `gehostet` für Extrahop-verwaltete Sensoren. | `sudo EXTRAHOP_CONNECTION_MODE=hosted rpm --install extrahop-key-forwarder.x86_64.rpm` |
| `EXTRAHOP_EDA_HOSTNAME` | Gibt den vollqualifizierten Domänenname des selbstverwalteten Sensor. | `sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c dpkg --install extrahop-key-forwarder_amd64.deb` |
| `EXTRAHOP_LOCAL_LISTENER_PORT` | Der Key-Forwarder empfängt Sitzungsschlüssel lokal aus der Java-Umgebung. über einen TCP-Listener auf localhost (127.0.0.1) und den im `LOCAL_LISTENER_PORT` Feld. Wir haben empfohlen, diesen Port beizubehalten auf den Standardwert 598 gesetzt. Wenn Sie die Portnummer ändern, müssen Sie die `-javaagent` Argument, um den neuen Port zu berücksichtigen. | `sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_LOCAL_LISTENER_PORT=900 rpm --install extrahop-key-forwarder.x86_64.rpm` |
| `EXTRAHOP_SYSLOG` | Gibt die Einrichtung oder den Maschinenprozess an, der das Syslog-Ereignis erzeugt hat. Das Standardeinrichtung ist `local3`, was ein Systemdaemon ist Prozesse. | `sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_SYSLOG=local1 dpkg --install extrahop-key-forwarder_amd64.deb` |
| `EXTRAHOP_ADDITIONAL_ARGS` | Gibt zusätzliche Optionen für die Schlüsselweiterleitung an. | `sudo EXTRAHOP_CONNECTION_MODE=hosted EXTRAHOP_ADDITIONAL_ARGS="-v=true -libcrypto=/some/path/libcrypto.so libcrypto=/some/other/path/libcrypto.so" rpm --install extrahop-key-forwarder.x86_64.rpm` |