Sitzungsschlüssel an von ExtraHOP verwaltete Sensoren weiterleiten

Veröffentlicht: 2024-07-02

Das ExtraHop-System kann den SSL/TLS-Verkehr in Ihrem Netzwerk mit weitergeleiteten Sitzungsschlüsseln von Ihren in AWS bereitgestellten Servern entschlüsseln. Die Weiterleitung von Sitzungsschlüsseln muss auf jedem von ExtraHOP verwalteten Gerät aktiviert sein Sensor, und Sie müssen auf jeder VPC, die die Server enthält , von denen Sie verschlüsselten Verkehr weiterleiten möchten, einen VPC-Endpunkt erstellen.

Kommunikation zwischen dem Schlüsselspediteur und dem Sensor ist mit TLS 1.2 verschlüsselt.

Erfahre mehr über SSL/TLS-Entschlüsselung.

Aktivieren Sie die Weiterleitung von Sitzungsschlüsseln in RevealX 360

Die Weiterleitung von Sitzungsschlüsseln kann aktiviert werden, wenn Sie ExtraHop-Managed bereitstellen Sensoren von RevealX 360. Sie müssen die Sitzungsschlüsselweiterleitung für jeden aktivieren Sensor.

1. Loggen Sie sich in die RevealX 360 Console ein.
2. Klicken Sie auf Systemeinstellungen und klicken Sie dann **Die gesamte Verwaltung**.
3. Klicken Sie **Sensoren einsetzen**. Wählen Sie die **Sitzungsschlüsselweiterleitung auf diesem Sensor aktivieren** Kontrollkästchen, wenn Sie den Bereitstellungsvorgang abschließen.
4. Aus dem Sensoren Seite, warten Sie, bis in der Spalte Status Aktiviert und in der Spalte Key Forwarding Endpunkt die Endpunktzeichenfolge angezeigt wird.
5. Kopieren Sie die Endpunktzeichenfolge. Die Zeichenfolge ist erforderlich, wenn Sie einen Endpunkt in Ihrer VPC erstellen.

Sicherheitsgruppen in AWS konfigurieren

Sicherheitsgruppen legen fest, welche Server Sitzungsschlüssel an den VPC-Endpunkt weiterleiten können und welche Sitzungsschlüssel vom VPC-Endpunkt akzeptiert werden. In den folgenden Schritten wird beschrieben, wie Sie die Sicherheitsgruppe erstellen, die eingehender Datenverkehr zu Ihrem VPC-Endpunkt zulässt.

Hinweis: Ihre AWS-Instances, die Sitzungsschlüssel weiterleiten, müssen mit einer Sicherheitsgruppe konfiguriert sein, die ausgehender Datenverkehr zum VPC-Endpunkt zulässt.

1. Melden Sie sich bei der AWS-Managementkonsole an.
2. In der Alle Dienste Abschnitt, unter Rechnen, klicken **EC2**.
3. Im linken Bereich unter Netzwerk und Sicherheit, klicken **Sicherheitsgruppen**.
4. klicken **Sicherheitsgruppe erstellen**.
5. Geben Sie einen Namen für die Sicherheitsgruppe ein.
6. Geben Sie eine Beschreibung der Sicherheitsgruppe ein.
7. Wählen Sie aus der Dropdownliste die VPC aus, von der Sie den Datenverkehr weiterleiten möchten. Sie müssen für jede VPC, für die Sie einen Endpunkt benötigen, eine Sicherheitsgruppe erstellen.
8. In der Regel für eingehenden Datenverkehr Abschnitt, klicken **Regel hinzufügen**, und füllen Sie die folgenden Felder aus:
   - **Typ:** Benutzerdefiniertes TCP
   - **Protokoll:** TCP

- **Portbereich:** 4873
- **Quelle:** Wählen **Benutzerdefiniert** aus der Dropdownliste und wählen Sie im nächsten Feld eine oder mehrere Optionen aus, z. B. den CIDR-Block für die VPC, einen CIDR-Block für den IP-Adressbereich, der alle Server umfasst, von denen Sie geheime Daten weiterleiten möchten, oder eine bestehende Sicherheitsgruppe, die sowohl den Instances als auch dem Endpunkt zugeordnet ist — die Sicherheitsgruppe muss ausgehenden Datenverkehr zulassen Verkehr zu TCP:4873.

9. klicken **Sicherheitsgruppe erstellen**.

Endpunkt in einer überwachten VPC erstellen

Erstellen Sie für jede VPC einen Endpunkt, der weitergeleitete Sitzungsschlüssel von Ihren Servern akzeptieren kann, und senden Sie sie an den VPC Endpoint Service im RevealX 360-System.

1. Kehren Sie zur AWS-Managementkonsole zurück.
2. In der Alle Dienstleistungen Abschnitt, unter Netzwerk- und Inhaltsbereitstellung, klicken **VPC**.
3. Im linken Bereich, unter Virtuelle private Cloud, klicken **Endpunkte**. (Klicken Sie nicht auf Endpoint Services.)
4. Klicken Sie **Endpunkt erstellen**.
5. Wählen Sie für die Kategorie Service **Service anhand des Namens finden**.
6. Fügen Sie die Endpunktzeichenfolge, die Sie von RevealX 360 kopiert haben, in das Feld Service Name ein.
7. Klicken Sie **Verifizieren**.
8. Aus dem VPC Wählen Sie in der Dropdownliste die VPC mit den ENIs aus, die den Datenverkehr zum Sensor spiegeln.
9. Stellen Sie sicher, dass die **DNS-Namen aktivieren** Das Kontrollkästchen ist ausgewählt.

   Wichtig: Sie müssen wählen **DNS-Hostnamen aktivieren** und **DNS-Unterstützung aktivieren** in den VPC-Einstellungen.

10. Wählen Sie die Sicherheitsgruppe aus, die Sie im vorherigen Verfahren konfiguriert haben.
11. Klicken Sie **Endpunkt erstellen**.
12. Wiederholen Sie diese Schritte, um für jede Ziel-ENI, die eine andere VPC ist, einen Endpunkt zu erstellen.

Installieren Sie die Sitzungsschlüsselweiterleitung auf Servern

In den folgenden Schritten wird beschrieben, wie Sie die ExtraHop Session Key Forwarder-Software auf unterstützten Windows- und Linux-Servern installieren und konfigurieren.

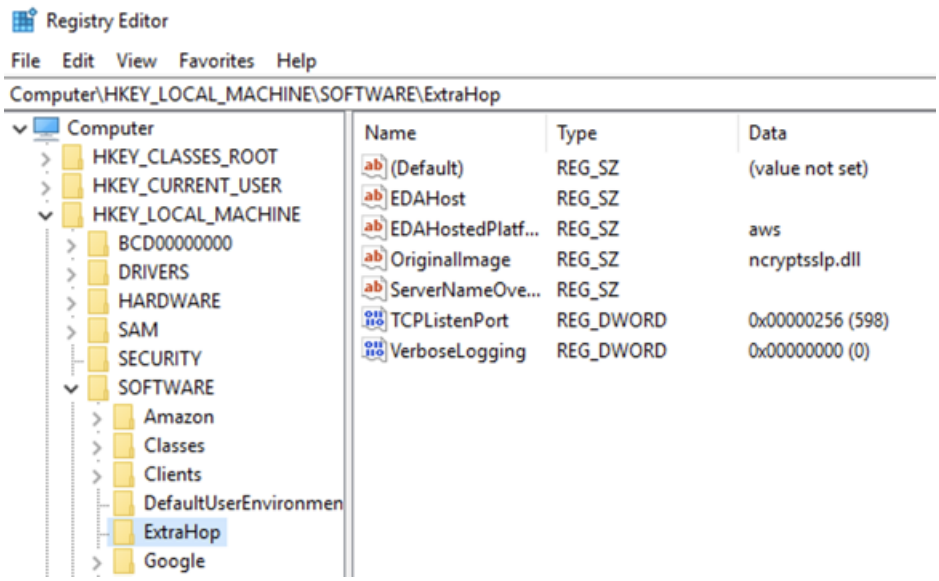
Bevor Sie beginnen

- Serverinstanzen müssen über ein Instanzprofil mit einer IAM-Rolle verfügen, das die Berechtigung zur Beschreibung von Traffic Mirror-Sitzungen (DescribeTrafficMirrorSessions) und Traffic MirrorZielen (DescribeTrafficMirrorTargets) gewährt. Weitere Informationen zum Erstellen eines Instance-Profils finden Sie in der AWS-Dokumentation, Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden.

Windows-Server

1. Melden Sie sich beim Windows-Server an.
2. Herunterladen die neueste Version der Session Key Forwarder-Software.
3. Doppelklicken Sie auf `ExtraHopSessionKeyForwarder.msi` Datei und Klick **Weiter**.

4. Wählen Sie das Kästchen aus, um die Bedingungen der Lizenzvereinbarung zu akzeptieren, und klicken Sie dann auf **Weiter**.
5. Auf dem Sensor Bildschirm Hostname, lassen Sie das Feld Hostname leer und klicken Sie dann auf **Weiter**.
6. Akzeptieren Sie den standardmäßigen TCP-Listen-Port-Wert 598 (empfohlen), oder geben Sie einen benutzerdefinierten Portwert ein, und klicken Sie dann auf **Weiter**.
7. klicken **Installieren**.
8. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertig stellen**, und klicken Sie dann **Nein** um den Serverneustart zu überspringen.
9. Öffnen Sie den Windows-Registrierungseditor.
10. Klicken Sie im Abschnitt Software von HKEY_LOCAL_MACHINE auf **ExtraHop**.
11. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle im rechten Bereich und wählen Sie **Neu** > **Zeichenkettenwert**.
12. Typ `Von EDA gehostete Plattform` im Namensfeld.
13. Doppelklicken **Von EDA gehostete Plattform** um den Zeichenkettenwert zu bearbeiten.
14. Typ `aws` in der Wert Datenfeld und dann klicken **OK**.
    Die Registrierung sollte der folgenden Abbildung ähneln.



15. Starten Sie den Server neu.

Debian-Ubuntu-Linux-Distributionen

1. Loggen Sie sich auf Ihrem Debian- oder Ubuntu-Linux-Server ein.
2. Herunterladen die neueste Version der ExtraHop Session Key Forwarder-Software.
3. Öffnen Sie eine Terminalanwendung und führen Sie den folgenden Befehl aus.

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

4. Wählen **gehostet**.
5. Wählen **Ok**, und drücken Sie dann die EINGABETASTE.

6. Geben Sie den folgenden Befehl ein, um sicherzustellen, dass `extrahop-key-forwarder` Dienst gestartet:

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

Die folgende Ausgabe sollte erscheinen:

```
Extrahop-key-forwarder.service - ExtraHop Session Key Forwarder Daemon
Loaded: loaded (/etc/rc.d/init.d/extrahop-key-forwarder; enabled; vendor
 preset: enabled)
Active: active (running) since Wed 2021-02-03 10:55:47 PDT; 5s ago
```

Wenn der Dienst nicht aktiv ist, starten Sie ihn, indem Sie diesen Befehl ausführen:

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

RPM-basierte Linux-Distributionen

1. Melden Sie sich bei Ihrem RPM-basierten Linux-Server an.
2. Herunterladen die neueste Version der ExtraHop Session Key Forwarder-Software.
3. Öffnen Sie eine Terminalanwendung und führen Sie den folgenden Befehl aus:

```
sudo EXTRAHOP_CONNECTION_MODE=hosted rpm --install <path to installer
 file>
```

4. Geben Sie den folgenden Befehl ein, um sicherzustellen, dass der Extrahop-key-forwarder-Dienst gestartet wurde:

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

Linux-Umgebungsvariablen

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

Variabel	Beschreibung	Beispiel
`EXTRAHOP_CONNECTION_MODE`	Gibt den Verbindungsmodus zum Sitzungsschlüsselempfänger an. Optionen sind `richten` für selbstverwaltete Sensoren und `gehostet` für von 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 in der `LOCAL_LISTENER_PORT` Feld. Wir haben empfohlen, für diesen Port den Standardwert	`sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_LOCAL_LISTENER_PORT=900 rpm --install extrahop-key-forwarder.x86_64.rpm`

Variabel	Beschreibung	Beispiel
	598 beizubehalten. Wenn Sie die Portnummer ändern, müssen Sie die `-javaagent` Argument, um den neuen Port zu berücksichtigen.	
`EXTRAHOP_SYSLOG`	Gibt die Einrichtung oder den Maschinenprozess an, der das Syslog-Ereignis ausgelöst hat. Die Standardeinrichtung ist `local3`, das sind System-Daemon-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`

Überprüfen Sie die Konfigurationseinstellungen

Um zu überprüfen, ob das ExtraHop-System weitergeleitete Schlüssel empfangen kann, erstellen Sie ein Dashboard, das erfolgreich empfangene Nachrichten identifiziert.

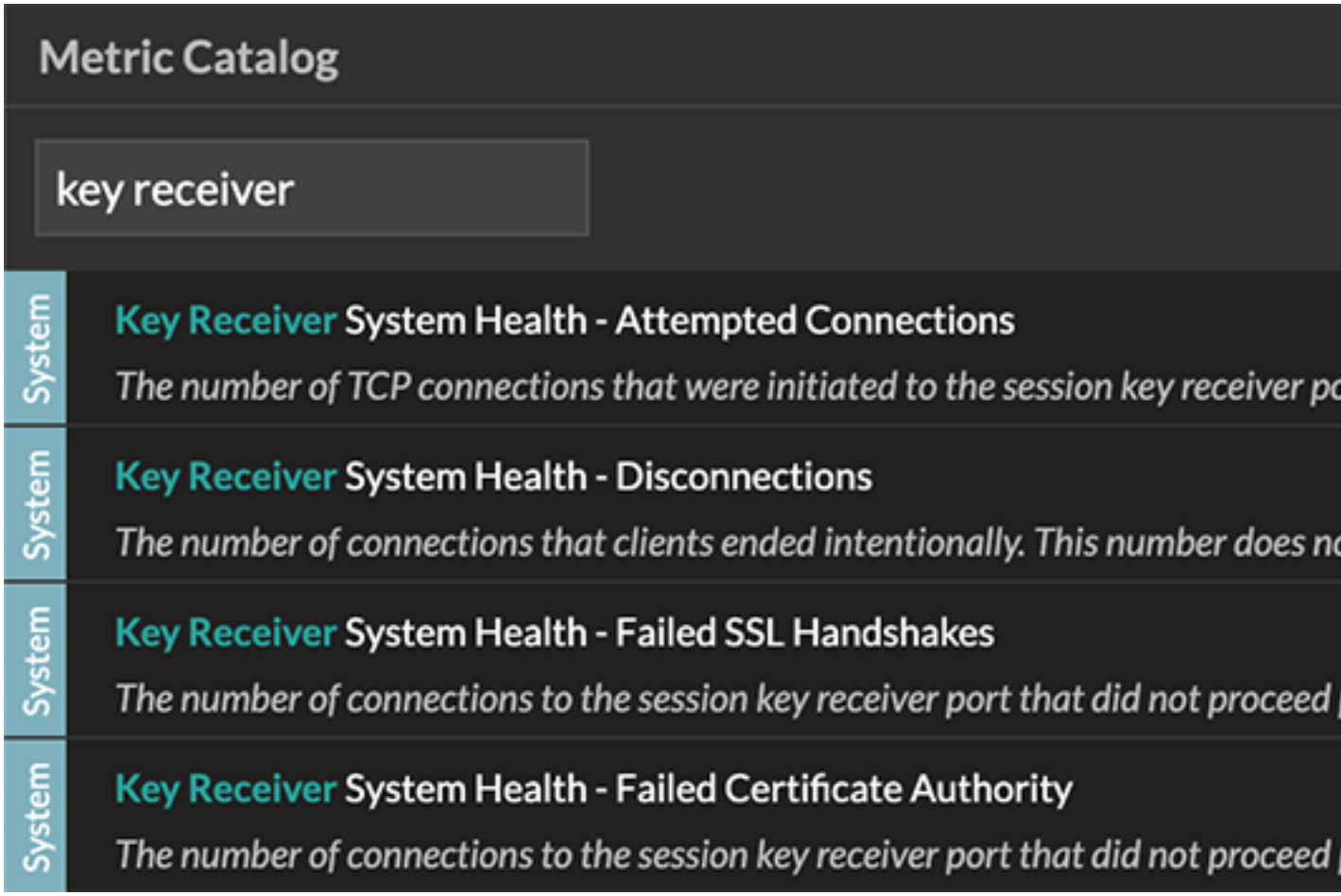
1. Erstellen Sie ein neues Dashboard.
2. Klicken Sie auf das Diagramm-Widget, um die Metrikquelle hinzuzufügen.
3. klicken **Quelle hinzufügen**.
4. In der Quellen Feld, Typ `Entdecke` im Suchfeld und dann wählen **Appliance entdecken**.
5. In der Metriken Feld, Typ `empfangene Nachrichten` im Suchfeld und dann wählen **Systemintegrität des Schlüsselempfängers — Empfangene Nachrichten mit Schlüsseln**.
6. klicken **Speichern**.

Das Diagramm wird mit der Anzahl der entschlüsselten Sitzungen angezeigt.

Zusätzliche Metriken zur Systemintegrität

Das ExtraHop-System bietet Metriken, die Sie zu einem Dashboard hinzufügen können, um den Zustand und die Funktionalität der Session Key Forwarder 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.



Erfahren Sie, wie Erstellen Sie ein Dashboard.