Forward session keys to ExtraHop-managed sensors

Published: 2022-09-27

The ExtraHop system can decrypt SSL/TLS traffic on your network with forwarded session keys from your servers deployed in AWS. Session key forwarding must be enabled on each ExtraHop-managed sensor, and you must create a VPC endpoint on each VPC that includes the servers that you want to forward encrypted traffic from.

Communication between the key forwarder and the sensor is encrypted with TLS 1.2.

Learn more about SSL/TLS decryption ⤤.

Enable session key forwarding in Reveal(x) 360

Session key forwarding can be enabled when you deploy ExtraHop-managed sensors from Reveal(x) 360. You must enable session key forwarding for each sensor.

1. Log in to the Reveal(x) 360 Console.
2. Click System Settings ⚙ and then click **All Administration**.
3. Click **Deploy Sensors**. Select the **Enable session key forwarding on this sensor** checkbox as you complete the deployment process.
4. From the Sensors page, wait for the Status column to display Enabled and the Key Forwarding Endpoint column to display the endpoint string.
5. Copy the endpoint string. The string is required when you create an endpoint in your VPC.

Configure security groups in AWS

Security groups determine which servers can forward session keys to the VPC endpoint as well as which session keys are accepted by the VPC endpoint. The following steps describe how to create the security group that permits inbound traffic to your VPC endpoint.

> 📝 **Note:** Your AWS instances that are forwarding session keys must be configured with a security group that allows outbound traffic to the VPC endpoint.

1. Log in to the AWS Management Console.
2. In the All services section, under Compute, click **EC2**.
3. In the left pane under Network & Security, click **Security Groups**.
4. Click **Create Security Group**.
5. Type a name for the security group.
6. Type a description about the security group.
7. From the drop-down list, select the VPC that you want to forward traffic from. You must create a security group for each VPC that you need an endpoint for.
8. In the Inbound rule section, click **Add rule**, and complete the following fields:

   - **Type:** Custom TCP
   - **Protocol:** TCP
   - **Port range:** 4873
   - **Source:** Select **Custom** from the drop-down list and in the next field select one or more options, such as the CIDR block for the VPC, a CIDR block for the range of IP addresses that includes all of the

servers that you want to forward secrets from, or an existing security group that is associated with both the instances and the endpoint—the security group must allow outbound traffic to TCP:4873.

9. Click **Create security group**.

Create endpoint in a monitored VPC

Create an endpoint for each VPC that can accept forwarded session keys from your servers and send them to the VPC Endpoint Service in the Reveal(x) 360 system.

1. Return to the AWS Management Console.
2. In the All services section, under Network & Content Delivery, click **VPC**.
3. In the left pane, under Virtual Private Cloud, click **Endpoints**. (Do not click Endpoint Services.)
4. Click **Create Endpoint**.
5. For the Service category, select **Find service by name**.
6. Paste the endpoint string you copied from Reveal(x) 360 into the Service Name field.
7. Click **Verify**.
8. From the VPC drop-down list, select the VPC that has the ENIs that are mirroring traffic to the sensor.
9. Make sure that the **Enable DNS name** checkbox is selected.

   (!) **Important:** You must select **Enable DNS hostnames** and **Enable DNS Support** in the VPC settings.

10. Select the security group you configured in the previous procedure.
11. Click **Create endpoint**.
12. Repeat these steps to create an endpoint for each target ENI that is a different VPC.

Install session key forwarding on servers

The following steps describe how to install and configure the ExtraHop session key forwarder software on supported Windows and Linux servers.

Before you begin

- Server instances must have an instance profile with an IAM role that grants permission to describe traffic mirror sessions (DescribeTrafficMirrorSessions) and traffic mirror targets (DescribeTrafficMirrorTargets). For more information about creating an instance profile, see the AWS documentation, Using an IAM role to grant permissions to applications running on Amazon EC2 instances ⧉.

Windows Server

1. Log in to the Windows server.
2. Download ⧉ the latest version of the session key forwarder software.
3. Double-click the `ExtraHopSessionKeyForwarder.msi` file and click **Next**.
4. Select the box to accept the terms of the license agreement and then click **Next**.
5. On the sensor hostname screen, leave the hostname field empty and then click **Next**.
6. Accept the default TCP listen port value of 598 (recommended), or type a custom port value and then click **Next**.
7. Click **Install**.
8. When the installation completes, click **Finish**, and then click **No** to skip the server reboot.
9. Open the Windows Registry Editor.
10. In the Software section of HKEY_LOCAL_MACHINE, click **ExtraHop**.

11. Right-click anywhere in the right pane and select **New** > **String Value**.
12. Type `EDAHostedPlatform` in the name field.
13. Double-click **EDAHostedPlatform** to edit the string value.
14. Type `aws` in the Value data field and then click **OK**.
    The registry should appear similar to the following figure.
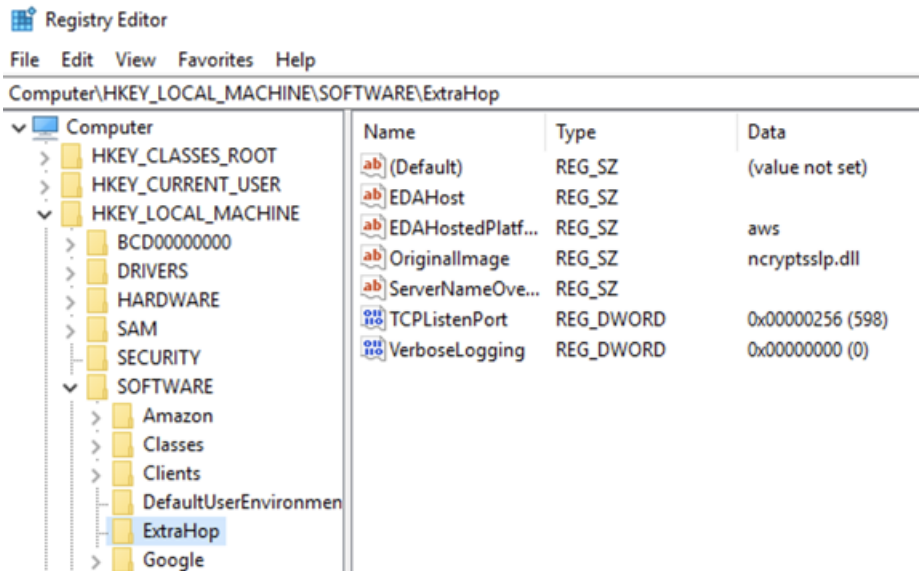
15. Reboot the server.

Debian-Ubuntu Linux distributions

1. Log in to your Debian or Ubuntu Linux server.
2. Download ⧉ the latest version of the ExtraHop session key forwarder software.
3. Open a terminal application and run the following command.

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

4. Select **hosted**.
5. Select **Ok**, and then press ENTER.
6. Type the following command to ensure that the `extrahop-key-forwarder` service started:

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

The following output should appear:

```
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
```

If the service is not active, start it by running this command:

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

RPM-based Linux distributions

1. Log in to your RPM-based Linux server.

2. Download ⬀ the latest version of the ExtraHop session key forwarder software.
3. Open a terminal application and run the following command:

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

4. Type the following command to ensure the extrahop-key-forwarder service started:

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

Linux environment variables

The following environment variables enable you to install the session key forwarder without user interaction.

Variable	Description	Example
EXTRAHOP_CONNECTION_MODE	Specifies the connection mode to the session key receiver. Options are direct for self-managed sensors and hosted for ExtraHop-managed sensors.	sudo EXTRAHOP_CONNECTION_MODE=hosted rpm --install extrahop-key-forwarder.x86_64.rpm
EXTRAHOP_EDA_HOSTNAME	Specifies the fully qualified domain name of the self-managed sensor.	sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c dpkg --install extrahop-key-forwarder_amd64.deb
EXTRAHOP_LOCAL_LISTENER_PORT	The key forwarder receives session keys locally from the Java environment through a TCP listener on localhost (127.0.0.1) and the port specified in the LOCAL_LISTENER_PORT field. We recommended that this port remain set to the default of 598. If you change the port number, you must modify the -javaagent argument to account for the new port.	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	Specifies the facility, or machine process, that created the syslog event. The default facility is local3, which is system daemon processes.	sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_SYSLOG=local1 dpkg --install extrahop-key-forwarder_amd64.deb
EXTRAHOP_ADDITIONAL_ARGS	Specifies additional key forwarder options.	sudo EXTRAHOP_CONNECTION_MODE=hosted EXTRAHOP_ADDITIONAL_ARGS="-v=true -libcrypto=/some/path/libcrypto.so libcrypto=/some/other/path/libcrypto.so" rpm

Variable	Description	Example
		`--install extrahop-key-` `forwarder.x86_64.rpm`

Validate the configuration settings

To validate that the ExtraHop system is able to receive forwarded keys, create a dashboard that identifies messages successfully received.

1. Create a new dashboard.
2. Click the chart widget to add the metric source.
3. Click **Add Source**.
4. In the Sources field, type `Discover` in the search field and then select **Discover Appliance**.
5. In the Metrics field, type `received messages` in the search field and then select **Key Receiver System Health - Received Messages Containing Keys**.
6. Click **Save**.

The chart appears with a count of decrypted sessions.

Additional system health metrics

The ExtraHop system provides metrics that you can add to a dashboard to monitor session key forwarder health and functionality.

To view a list of available metrics, click the System Settings icon ⚙ and then click **Metric Catalog**. Type `key receiver` in the filter field to display all available key receiver metrics.

Metric Catalog

key receiver

System	**Key Receiver** System Health - Attempted Connections *The number of TCP connections that were initiated to the session key receiver po*
System	**Key Receiver** System Health - Disconnections *The number of connections that clients ended intentionally. This number does n*
System	**Key Receiver** System Health - Failed SSL Handshakes *The number of connections to the session key receiver port that did not proceed*
System	**Key Receiver** System Health - Failed Certificate Authority *The number of connections to the session key receiver port that did not proceed*

Learn how to Create a dashboard ⤢.