Install the ExtraHop session key forwarder on a Linux server

Published: 2020-10-27

Perfect Forward Secrecy (PFS) is a property of secure communication protocols that enables short-term, completely private session key exchanges between clients and servers. When the session keys are only shared between the client and server, the Discover appliance is unable to decrypt this traffic, even when the Discover appliance has a copy of the server private key. The only way for the Discover appliance to decrypt this traffic is to get a copy of the session key from the server.

ExtraHop offers session key forwarding software for Windows and Linux that you can install on your servers that are sending SSL-encrypted traffic. The forwarder sends the SSL sessions keys to your ExtraHop Discover appliance. The session keys then enable the Discover appliance to decrypt those SSL/TLS sessions in your data feed. The ExtraHop session key forwarder decrypts sessions through the Microsoft Secure Channel (Schannel) security package, Java SSL/TLS (Java versions 6 through 10), and dynamically linked OpenSSL (1.0.x and 1.1.x) libraries. OpenSSL is only supported on Linux with kernel versions 4.4 and later or RHEL 7.6 and later.

Depending on your environment, you can configure the Discover appliance for session key forwarding with or without a server certificate and private keys.

- (Recommended) If your environment does not require a server certificate, you can disable the private key requirement and configure global port mappings for the protocol traffic you want to decrypt.
- If your environment requires a server certificate, first complete the steps in the Decrypt SSL traffic with certificates and private keys guide, and then complete the steps below to install the forwarder software.

Before you begin

- Review the list of supported cipher suites that can be decrypted by the Discover appliance when session key forwarding is configured.
- Make sure that the Discover appliance is licensed for SSL Decryption and SSL Shared Secrets.

  Note: The ExtraHop system cannot decrypt TLS-encrypted TDS traffic through session key forwarding. Instead, you can upload an RSA private key.

- Install the session key forwarder on RHEL, CentOS, Fedora, or Debian-Ubuntu Linux distributions. The session key forwarder might not function correctly on other distributions.

Enable the SSL session key receiver service

You must enable the session key receiver service on the Discover appliance before the appliance can receive and decrypt sessions keys from the session key forwarder. By default, this service is disabled.

1. Log into the Admin UI on the Discover appliance.
2. In the Appliance Settings section, click **Services**.
3. Select the **SSL Session Key Receiver** checkbox.
4. Click **Save**.

Add a global port to protocol mapping

Add each protocol for the traffic that you want to decrypt with your session key forwarders.

1. Log into the Admin UI on the Discover appliance.
2. In the System Configuration section, click **Capture**.
3. Click **SSL Decryption**.

4. In the Private Key Decryption section, clear the Require Private Keys checkbox.
5. In the Global Protocol to Port Mapping section, click **Add Global Protocol**.
6. From the Protocol drop-down list, select the protocol for the traffic that you want to decrypt.
7. In the Port field, type the number of the port. Type `0` to add all ports.
8. Click **Add**.

Install the software

For RPM-based Linux distributions

1. Log into 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 rpm --install <path to installer file>
```

4. Open the initialization script in a text editor (vi or vim, for example).

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

5. In the `EDA_HOSTNAME` field, type the name of your Discover appliance, similar to the following example.

```
#TODO:Type your Discover appliance hostname in the EDA_HOSTNAME field
EDA_HOSTNAME="discover.example.com"
```

6. Optional: 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.
7. Optional: If you prefer that syslog writes to a different facility than "local3" for key forwarder log messages, you can edit the `SYSLOG` field.
   The contents of the `extrahop-key-forwarder.conf` file should appear similar to the following example:

```
# TODO: Type your Discover appliance hostname in the EDA_HOSTNAME field
EDA_HOSTNAME="eda-prod.example.com"
LOCAL_LISTENER_PORT=598
SYSLOG="local3"
ADDITIONAL_ARGS=
```

8. Save the file and exit the text editor.
9. Start the `extrahop-key-forwarder` service:

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

For Debian-Ubuntu Linux distributions

1. Log into 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. In the package configuration window, type the fully qualified domain name or IP address of the ExtraHop Discover appliance where session keys will be forwarded and then press ENTER.

Tip: You can configure optional parameters LOCAL_LISTENER_PORT and SYSLOG by editing the `/opt/extrahop/etc/extrahop-key-forwarder.conf` file.

The contents of the `extrahop-key-forwarder.conf` file will appear similar to the following example:

```
EDA_HOSTNAME="eda-prod.example.com"
LOCAL_LISTENER_PORT=598
SYSLOG="local3"
ADDITIONAL_ARGS=
```

5. Ensure that the `extrahop-key-forwarder` service started:

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

The following output should appear:

```
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
```

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

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

Integrate the forwarder with the Java-based SSL application

The ExtraHop session key forwarder integrates with Java applications through the `-javaagent` option. Consult your application's specific instructions for modifying the Java runtime environment to include the `-javaagent` option.

As an example, many Tomcat environments support customization of Java options in the `/etc/default/tomcat7` file. In the following example, adding the `-javaagent` option to the JAVA_OPTS line causes the Java runtime to share SSL session secrets with the key forwarder process, which then relays the secrets to the Discover appliance so that the secrets can be decrypted.

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

Validate and troubleshoot your installation

If your Linux server has network access to the Discover appliance and the server SSL configuration trusts the certificate presented by the Discover appliance that you specified when you installed the session key forwarder, then the configuration is complete.

In cases where you might have problems with the configuration, the session key forwarder binary includes a test mode you can access from the command-line to test your configuration.

1. Log into your Linux server.
2. To validate your installation, perform an initial test by running the following command:

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

The following output should appear:

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

If there is a configuration issue, troubleshooting tips appear in the output to help you correct the issue. Follow the suggestions to resolve the issue and then run the test again.

3. You can optionally test the certificate path and server name override by adding the following options to the command above.

   - Specify this option to test the certificate without adding it to the certificate store.

     ```
     -cert <path to certificate>
     ```

   - Specify this option to test the connection if there is a mismatch between the Discover appliance hostname that the forwarder knows (SERVER) and the common name (CN) that is presented in the SSL certificate of the Discover appliance.

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

(Optional) Configure a server name override

If there is a mismatch between the Discover appliance hostname that the forwarder knows (SERVER) and the common name (CN) that is presented in the SSL certificate of the Discover appliance, then the forwarder must be configured with the correct CN.

We recommend that you regenerate the SSL self-signed certificate based on the hostname from the SSL Certificate section of the Admin UI instead of specifying this parameter.

1. Log into your Linux server.
2. Open the configuration file in a text editor.

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

3. Add a `SERVER_NAME_OVERRIDE` parameter with a value of the name found in the Discover appliance SSL certificate, similar to the following example:

   ```
   SERVER_NAME_OVERRIDE=altname.example.com
   ```

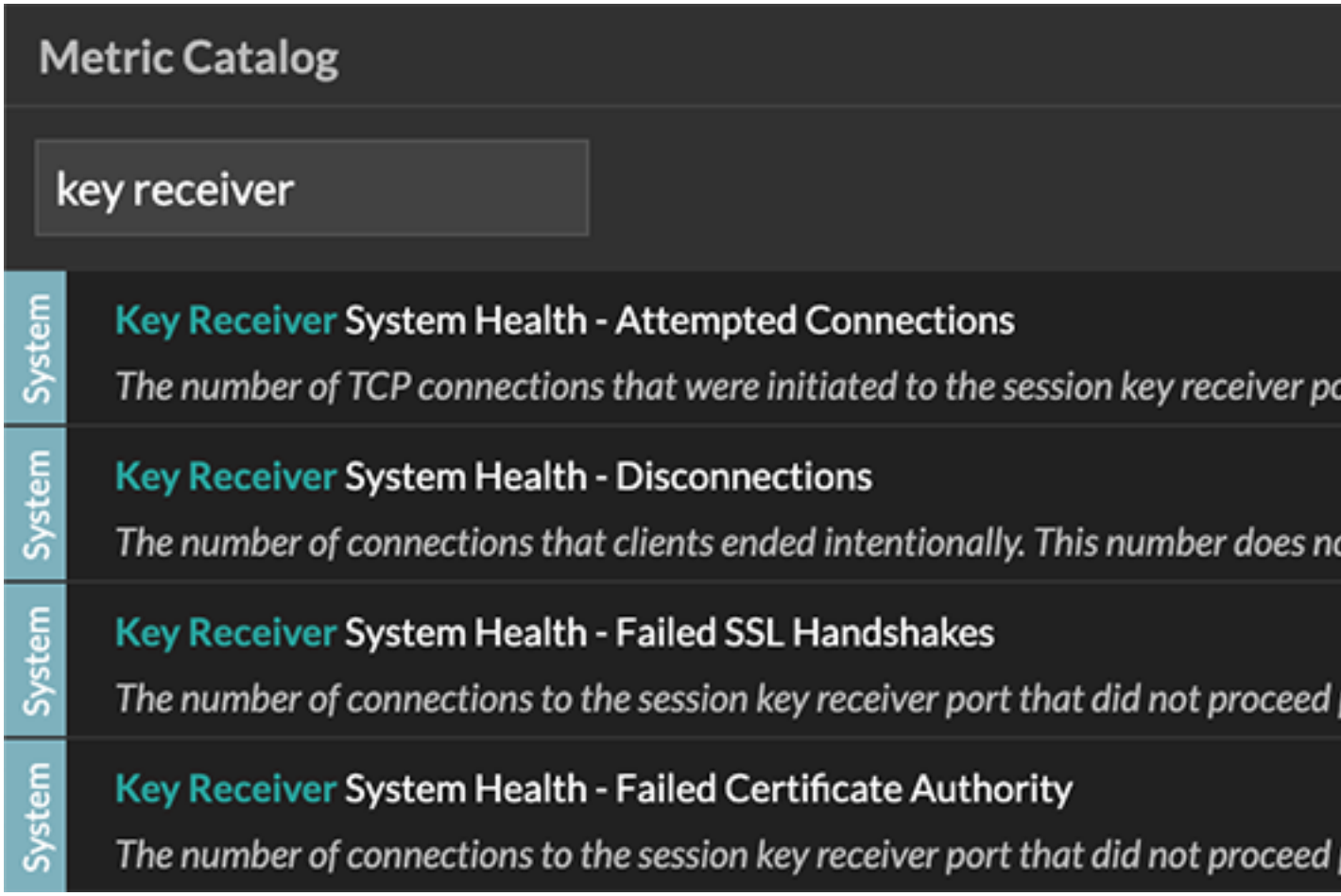
4. Save the file and exit the text editor.
5. Start the `extrahop-key-forwarder` service.

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

Key receiver system health metrics

The ExtraHop system provides key receiver metrics that you can add to a dashboard chart to monitor key receiver 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.



Tip: To learn how to create a new dashboard chart, see Edit a chart with the Metric Explorer.

View connected session key forwarders

You can view recently connected session key forwarders after you install the session key forwarder on your server and enable the SSL session key receiver service on the Discover appliance. Note that this page only displays session key forwarders that have connected over the last few minutes, not all session key forwarders that are currently connected.

1. Log into the Admin UI on the Discover appliance.
2. In the System Configuration section, click **Capture**.
3. Click **SSL Shared Secrets**.

Uninstall the software

If you no longer want the ExtraHop session key forwarder software installed, complete the following steps.

1. Log into the Linux server.
2. Open a terminal application and choose one of the following options to remove the software.
   - For RPM-based servers, run the following command:

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

- For Debian and Ubuntu servers, run the following command:

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

Type `Y` at the prompt to confirm the software removal and then press ENTER.

3. Click **Yes** to confirm.
4. After the software is removed, click **Yes** to restart the system

Common error messages

Errors created by the session key forwarder are logged to the Linux system log file.

Message	Cause	Solution
`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`	The monitored server cannot route any traffic to the Discover appliance.	Ensure firewall rules allow connections to be initiated by the monitored server to TCP port 4873 on the Discover appliance.
`connect: dial tcp <IP address>:4873: connectex: No connection could be made because the target machine actively refused it`	The monitored server can route traffic to the Discover appliance, but the receiving process is not listening.	Ensure that the Discover appliance is licensed for both the SSL Decryption and SSL Shared Secrets features.
`connect: x509: certificate signed by unknown authority`	The monitored server is not able to chain up the Discover appliance certificate to a trusted Certificate Authority (CA).	Ensure that the Linux certificate store for the computer account has trusted root certificate authorities that establish a chain of trust for the Discover appliance.
`connect: x509: cannot validate certificate for <IP address> because it doesn't contain any IP SANs`	An IP address was supplied as the `SERVER` parameter when installing the forwarder, but the SSL certificate presented by the Discover appliance does not include an IP address as a Subject Alternate Name (SAN).	Select from the following three solutions. • Replace the IP address for the `SERVER` value in the `/etc/init.d/extrahop-key-forwarder` file with a hostname. The hostname must match the subject name in the Discover appliance certificate. • If the server is required to connect to the Discover appliance by IP address, uninstall and reinstall the forwarder, specifying the subject name from the

Message	Cause	Solution
		Discover appliance certificate as the value of `server-name-override`.
		• Re-issue the Discover appliance certificate to include an IP Subject Alternative Name (SAN) for the given IP address.

Supported SSL cipher suites

To decrypt SSL traffic in real time, you must configure your server applications to encrypt traffic with supported ciphers. The following information provides a list of supported cipher suites and the best practices you should consider when implementing SSL encryption.

- Turn off SSLv2 to reduce security issues at the protocol level.
- Turn off SSLv3, unless required for compatibility with older clients.
- Turn off SSL compression to avoid the CRIME security vulnerability.
- Turn off session tickets unless you are familiar with the risks that might weaken Perfect Forward Secrecy.
- Configure the server to select the cipher suite in order of the server preference.

The following cipher suites can be decrypted by the ExtraHop appliance and are listed in from strongest to weakest and by server preference:

- AES256-GCM-SHA384
- AES128-GCM-SHA256
- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DES-CBC3-SHA

The following list includes some common cipher suites that support Perfect Forward Secrecy (PFS) and can be decrypted by the ExtraHop appliance when session key forwarding is configured. To configure session key forwarding, see Install the ExtraHop session key forwarder on a Windows server or Install the ExtraHop session key forwarder on a Linux server.

- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-ECDSA-RC4-SHA
- ECDHE-ECDSA-DES-CBC3-SHA

The following list of cipher suites support Perfect Forward Secrecy (PFS) but cannot be decrypted by the ExtraHop appliance:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES128-SHA256

Session key forwarder options

You can configure the session key forwarder by editing the `extrahop-key-forwarder.conf` file.

The table below lists all of the configurable options.

Important: If you add options to `extrahop-key-forwarder.conf` that do not have dedicated variables, they must be in the `ADDITIONAL_ARGS` field. For example:

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

Option	Description
`-cert <path>`	Specifies the path to the server certificate. Only specify this option if the server certificate is not signed by a trusted certificate authority.
`-elevated`	Runs the key forwarder with elevated privileges.
`-go-binary <value>`	Specifies glob patterns to find Go binaries. This option can be specified multiple times.
`-hearbeat-interval`	Specifies the time interval in seconds between heartbeat messages. The default interval is 30 seconds.
`-libcrypto <path>`	Specifies the path to the OpenSSL library, `libcrypto`. This option can be specified multiple times if you have multiple installations of OpenSSL.
`-openssl-discover`	Automatically discovers `libcrypto` implementations. The default value is "true". You must type `-openssl-discover=false` to disable OpenSSL decryption.
`-pidfile <path>`	Specifies the file where this server records its process ID (PID).

Option	Description
`-port <value>`	Specifies the TCP port that the Discover appliance is listening on for forwarded session keys. The default port is 4873.
`-server <string>`	Specifies the fully qualified domain name of the ExtraHop Discover appliance.
`-server-name-override <value>`	Specifies the subject name from the Discover appliance certificate. Specify this option if this server can only connect to the Discover appliance by IP address.
`-syslog <facility>`	Specifies the facility sent by the key forwarder. The default facility is local3.
`-t`	Perform a connectivity test. You must type `-t=true` to run with this option.
`-tcp-listen-port <value>`	Specifies the TCP port that the key forwarder is listening on for forwarded session keys.
`-username <string>`	Specifies the user that the session key forwarder runs under after the forwarder software is installed.
`-v`	Enable verbose logging. You must type `-v=true` to run with this option.