Install the ExtraHop session key forwarder on a Linux server

Published: 2018-07-07

The ExtraHop session key forwarder runs as a process on a monitored Linux server running SSL services. The forwarder establishes an SSL-secured connection to an ExtraHop Discover appliance to send all SSL session keys through. The session keys enable the Discover appliance to decrypt SSL/TLS sessions encrypted with Perfect Forward Secrecy (PFS) ciphers.

Before you begin

- Read our blog post: What is Perfect Forward Secrecy?
- 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 running firmware version 7.1 or later.
- Make sure that the Discover appliance is licensed for SSL Decryption.
- Install the session key forwarder on one or more Linux servers, either a Debian-based Linux distribution or an RPM-based Linux distribution with a Java-based encryption framework.
- Session key processing on the Discover appliance requires that you upload the server certificate and private key file for any monitored SSL-encrypted service to the Discover appliance. Go to the **Capture** > **SSL Decryption Keys** page in the Admin UI to upload a .pem file that includes both a private key and certificate. You can also upload a password-protected PKCS#12 (.PFX) file.
- Make sure that the server certificates have an RSA public key. DSA and ECDSA public keys are not currently supported.
- The session key forwarder on the Linux server must be able to access a trusted CA certificate from the Linux trust store to validate the certificate (or chain of certificates) that the Discover appliance presents.
- The traffic for each monitored SSL server must be part of the data feed to the Discover appliance.

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.

   If you do not see the checkbox, and you have purchased the SSL Decryption license, contact ExtraHop Support to update your license.
4. Click **Save**.

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.
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.

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 -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:

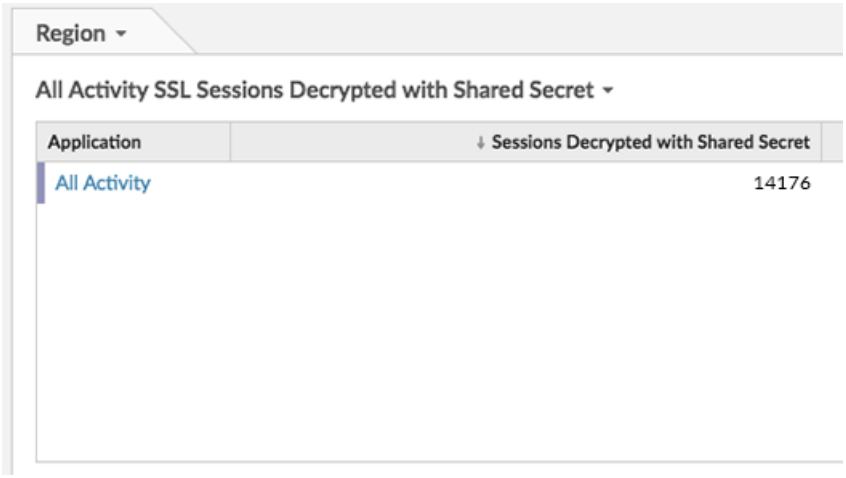
   ```
   SERVER_NAME_OVERRIDE=altname.example.com
   ```

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

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

Create a dashboard to see sessions decrypted with a shared secret

When the Discover appliance receives session keys and applies them to decrypted sessions, the Shared Secret metric counter (in **Applications** > **All Activity** > **SSL Sessions Decrypted**) is incremented. Create a dashboard chart with this metric to see if the Discover appliance is successfully receiving session keys from the monitored servers.



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 SSL connections to be initiated from the monitored server to 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. • If there is a hostname that the server can connect to the Discover appliance with, and that hostname matches the subject name in the Discover appliance certificate, edit the `/etc/init.d/extrahop-key-forwarder` file, specifying that hostname as the value of SERVER. • If the server is required to connect to the Discover appliance by IP address, uninstall and reinstall the forwarder, specifying the

Message	Cause	Solution
		subject name from the 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.