SSL/TLS decryption

Published: 2023-07-10

Encrypting sensitive data is a critical part of protecting your network assets; however, encryption also decreases visibility into the network for cybersecurity and forensics. Because encrypted traffic is an increasingly common vector for malicious activity, we recommend that you configure the ExtraHop system to decrypt your critical SSL/TLS traffic to enable detections that can identify suspicious behaviors and potential attacks.

The following requirements must be met for SSL/TLS decryption:

- Your SSL/TLS server traffic must be encrypted with a supported cipher suite.
- You can only decrypt traffic for the services that you provide and control on your network.

Encryption types

When a client initiates a connection to a server over SSL/TLS, a series of handshake exchanges identify the cipher suite that includes the set of algorithms that encrypts the data and authenticates the data integrity.

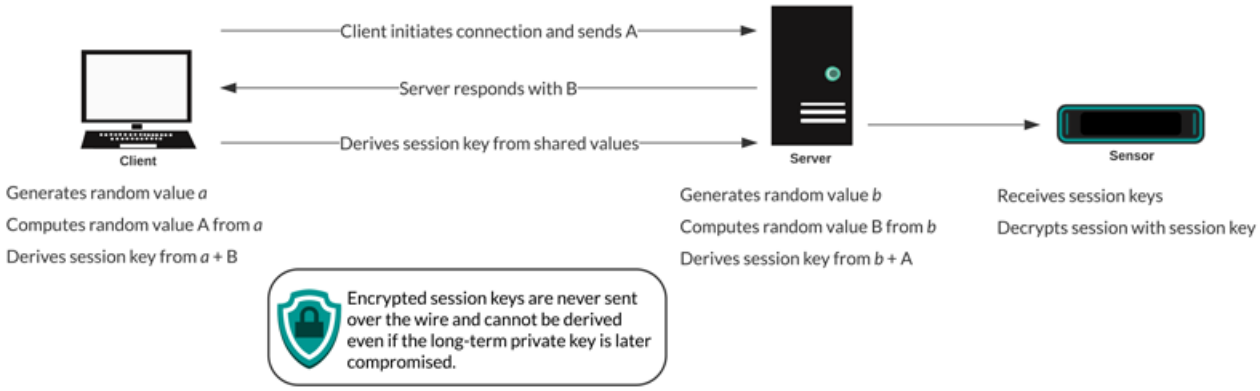
You can configure the ExtraHop system to decrypt SSL/TLS traffic based on the type of supported cipher suite that the network connection is secured with.

Video: Learn more about encryption.

Session key forwarding

When session key forwarding is enabled on the ExtraHop system, a light-weight agent can be installed on the server to forward session keys to the system and the system is able to decrypt the related SSL/TLS traffic. Communication between the key forwarder and the system is encrypted with TLS 1.2.

Perfect Forward Secrecy (PFS) cipher suites mutually derive a session key through a series of exchanges between the client and server—only the client and server know the session key, which is never sent over the wire network. Even if the long-term server key is compromised, the ephemeral session key remains secure.



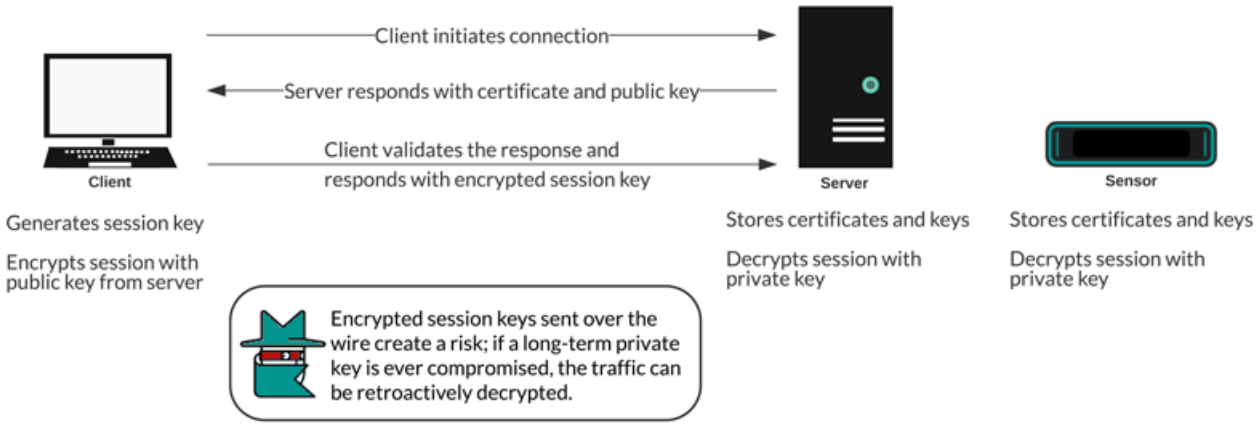
Certificates and keys

When a certificate and private key for supported cipher suites are uploaded to an ExtraHop system, the system is able to decrypt the related SSL/TLS traffic.

Note: TLS 1.2 and earlier support RSA for the key exchange, but TLS 1.3 does not.

Cipher suites for RSA can be decrypted with a server certificate and private key. When a client connects to a server over SSL/TLS, the server responds with a certificate that validates its identity and shares the public key. The client generates and encrypts a session key and sends the encrypted session key to the server. The client validates that the certificate is signed by a trusted certificate authority and that the server matches the requested domain.

Because the encrypted session key is sent over the wire network during the handshake and the private key is held long term on the server, anyone with access to the traffic, the server certificate, and the private key can derive the session key and decrypt the data. Teams that are responsible for encrypting their traffic might be hesitant to share private keys with other devices on the network to minimize risk.



Best practices

Here are some best practices you should consider when implementing SSL/TLS encryption.

- Turn off SSLv2 to reduce security issues at the protocol level.
- Turn off SSLv3, unless it is 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.
- Note that session key forwarding is the only option for traffic encrypted with TLS 1.3.

Which traffic to decrypt

The traffic you want to inspect is likely to contain sensitive data, so the ExtraHop system does not write decrypted payload data to disk. The ExtraHop system analyzes the traffic in real-time and then discards the session key unless a Trace appliance is deployed for continuous packet capture. Optionally, the system can be configured to store the session key with the packets, which is a safer approach than sharing the long-term private key with analysts.

Here are some examples of the type of data you should consider decrypting with the ExtraHop system:

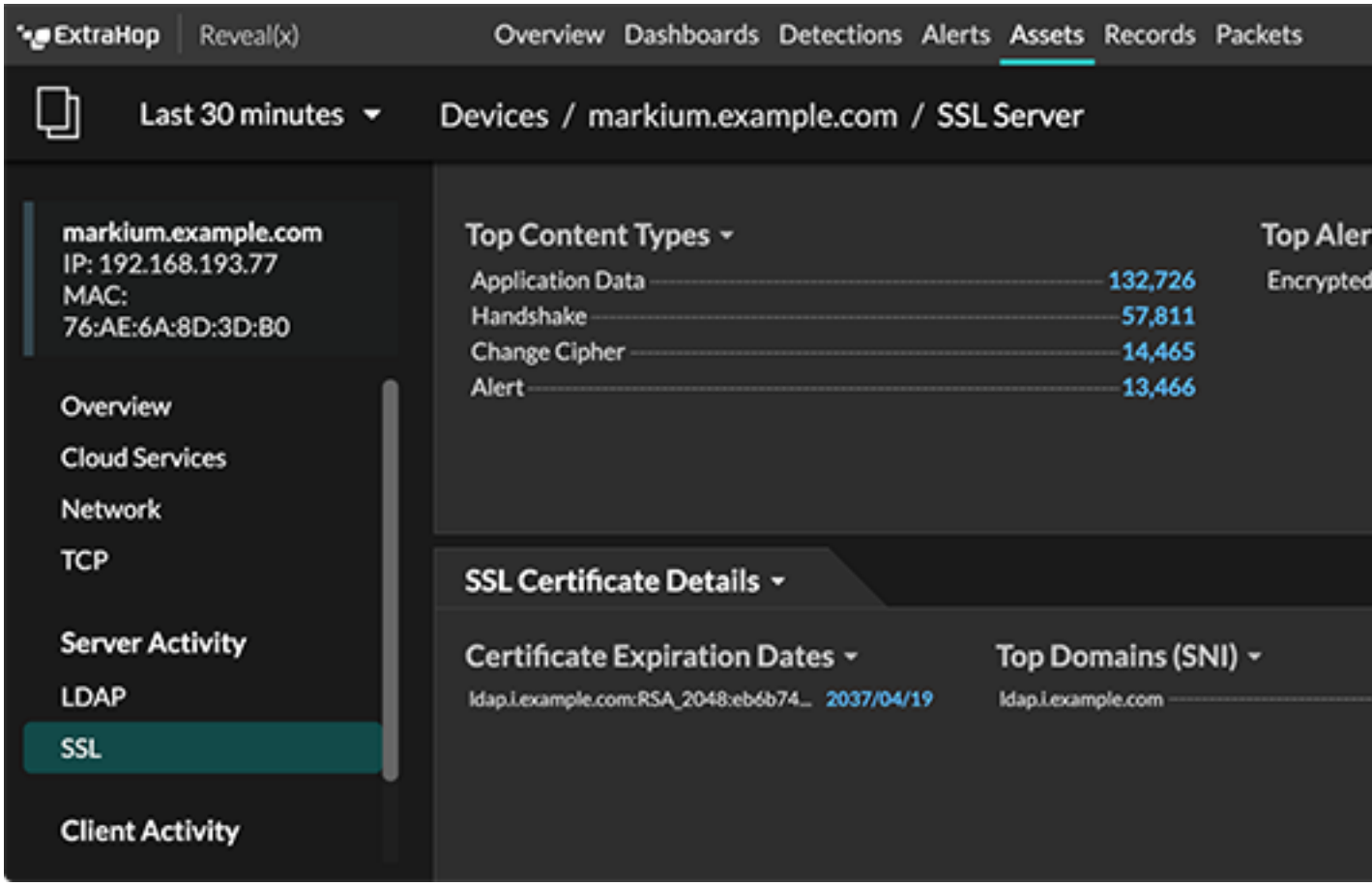
- Decrypting secure HTTP (HTTPS) traffic exchanged between a web server and client through an SSL/TLS connection can surface web application attacks such as SQL injection (SQLi) and cross-site scripting (XSS), which are among the most common web application security risks on the OWASP Top 10 list. Decrypting HTTPS traffic can also surface exploit mechanisms, for example a malicious URI or query parameter, for common vulnerabilities and exposures (CVEs) in web applications and servers.
- Decrypting secure LDAP (LDAPS) traffic exchanged between an LDAP server and a client through an SSL/TLS connection can surface reconnaissance activity. For example, the BloodHound attack tool encrypts LDAP queries with SSL/TLS (as well as Kerberos or NTLM) to collect large lists of Active

Directory objects for reconnaissance. Decrypting LDAPS traffic can also surface the exploit mechanism for the critical CVE referred to as Log4Shell.

- Decrypting MySQL, PostgreSQL, MS SQL Server, or Oracle database traffic exchanged between a database server and a client through an SSL/TLS connection can surface malicious statements or commands that are intended to delete, modify, or read data.
- Decrypting traffic that you might need for forensic auditing helps to meet compliance regulations or investigate incidents on critical systems—such as your customer databases, systems that house valuable intellectual property, or servers that provide critical network services.

You can also identify the type of encrypted traffic for a specific device discovered by the ExtraHop system. Find the device in the system and navigate to the device detail page.

In the left pane, click **SSL** in the Server Activity section. In the center pane, scroll to the Top Cipher Suites chart.



How to decrypt your SSL traffic

How you decrypt SSL traffic depends on the cipher suite and your server implementation.

Note: See supported cipher suites to learn which cipher suites can be decrypted and their requirements.

If your SSL traffic is encrypted with PFS cipher suites, you can install the ExtraHop session key forwarder software on each server that has the SSL traffic that you want to decrypt. The session key is forwarded to the ExtraHop system and the traffic can be decrypted. Note that your servers must support the session key forwarder software.

- Install the ExtraHop session key forwarder on a Windows server

- Install the ExtraHop session key forwarder on a Linux server

If you have an F5 load balancer, you can share session keys through the balancer and avoid installing the session key forwarding software on each server.

- Session key forwarding from an F5 LTM

If your SSL traffic is encrypted with RSA cipher suites, you can still install session key forwarder software on your servers (recommended). Alternatively, you can upload the certificate and private key to the ExtraHop system

- Decrypt SSL traffic with certificates and private keys

We recommend that you only decrypt the traffic that you need. You can configure the ExtraHop system to decrypt only specific protocols and map protocol traffic to non-standard ports.

- Add encrypted protocols
- Add global port to protocol mapping

Decrypting packets for forensic audits

If you have a Trace appliance or other packetstore configured, you can store session keys on the Trace appliance and you can download session keys with packet captures so that you can decrypt the packets in a packet analysis tool such as Wireshark. These options enable you to securely decrypt traffic without sharing long-term private keys with analysts.

The system only stores session keys for packets on disk—as packets are overwritten, the related stored session keys are deleted. Only session keys for decrypted traffic are sent to the Trace appliance for storage. The ExtraHop system sends the session key with the associated flow information to the Trace appliance. If a user has packets and session key privileges, the session key is provided when there is a matching flow in the queried time range. Extraneous session keys are not stored, and there is no limit to the number of session keys that the ExtraHop system can receive.

We recommend that you exercise caution when granting privileges to ExtraHop system users. You can specify the privileges that enable users to view and download packets or to view and download packets and stored session keys. Stored session keys should only be available to users who should have access to sensitive decrypted traffic. While the ExtraHop system does not write decrypted payload data to disk, access to session keys enables decryption of the related traffic. To ensure end to end security, the session keys are encrypted when moving between appliances as well as when the keys are stored on disk.

- Store SSL session keys on connected Trace appliances
- Download session keys with packet captures