Fact Sheet

Cogito Group

TLS interception

Safeguard the integrity and confidentiality of your data

Detect and block malicious elements, such as viruses and malware, and data leakage within encrypted connections

TLS interception allows for inspection to be done on secured traffic entering and exiting an environment.

What is TLS interception?

Transport Layer Security interception (TLS interception) involves intercepting encrypted connections to make them accessible for inspection. The intermediate stations that perform this activity are referred to as the 'TLS proxy'. TLS interception can be carried out for all types of TLS connections, such as HTTPS for web traffic and SMTP with STARTTLS for e-mail.

How does it work?

TLS is a protocol for setting up and using a cryptographically secured connection between two computer systems, a client and a server.

This safeguards the confidentiality and integrity of the content of the connection and authenticates the server so that the identity of the server cannot be falsified.

In the case of TLS interception, the TLS proxy intercepts the client's request to start an encrypted connection with the server and the TLS proxy acts as that particular server. Normally, this will not be accepted by the client because it is unable to correctly authenticate the identity of the server.

However, to enable the client to trust the TLS proxy, the root certificate (root CA) of the TLS proxy should be installed on the client.

The client will subsequently trust all certificates signed with this root certificate (root CA). For every server and corresponding domain name with which a client wishes to make a connection, the TLS proxy subsequently creates a certificate, the name of which corresponds to the domain requested, and which is signed by the root certificate (root CA) of the TLS proxy.

The client accepts the server certificate signed by the TLS proxy and sets up an encrypted connection with the TLS proxy. Next, the TLS proxy sets up an encrypted connection with the server and forwards the traffic between the client and the server. Since the TLS proxy is now located between the two encrypted connections, it can inspect and forward all traffic to the detection system. The detection system can be integrated in the TLS proxy or can be a separate appliance.

Inspection is only carried out at transport level. If an application,

such as malware, also applies separate encryption at application

level, the TLS proxy will usually not remove that encryption

What are the risks?

TLS proxies take over the role of clients of setting up secure connections with servers. Indeed, the TLS proxy will set up a secure connection with a server on the Internet instead of the end user's system. The TLS proxy will therefore need to perform all checks and provide all safeguards concerning the authentication of the server, as well as the confidentiality, integrity and authentication of the data transmitted and Client TLS proxy Server Detection received. The client software will subsequently only be able to rely on the TLS proxy when it comes to these aspects, without being able to verify them itself. In view of the large number of threats, modern browsers perform increasingly stringent checks on all these aspects, using wide-ranging security mechanisms.

To ensure the same level of security, the TLS proxy must perform the appropriate checks. Any weaknesses in this process could result in users' connections and the organisation's systems being manipulated or eavesdropped on.

TLS interception could prevent applications from making a connection with their server, if they only trust the specific certificate of that particular server rather than the alternative certificate of the TLS proxy. This measure is also known as certificate pinning.

Client authentication on the basis of a client certificate at the endpoint may also be impossible due to TLS interception. If applications use encryption algorithms or protocols that are not supported by the TLS proxy, connection problems could arise. This is mainly a risk for legacy applications but connection problems could also arise when new applications are introduced that use new encryption algorithms or protocols.6 Due to TLS interception, clients may also no longer be able to see that a certain website is using an extended validation certificate.7

Lastly, there is a risk that the TLS proxy will be hacked, since it is an extremely appealing target. If an attacker manages to compromise the TLS proxy, it will gain access to all the data flowing through it. The data in the TLS proxy is unencrypted and can therefore be viewed and altered by the attacker. The data may be confidential, such as passwords and financial information. Furthermore, an attacker who has stolen a TLS proxy root certificate can carry out man-in-the-middle attacks on clients who trust the certificate.

Safeguarding a TLS proxy

A TLS proxy is a valuable target and should in the majority of cases be regarded as one of the 'crown jewels' of your organisation.

The TLS proxy is capable of decrypting encrypted TLS traffic directed through the proxy and can therefore access the original data. If an attacker manages to compromise the TLS proxy or the private key of the root certificate, it can snoop on these data streams and moreover alter information. For this reason, it is vital to ensure that the TLS proxy itself is properly protected.

Follow these simple steps to ensure your TLS proxy is safeguarded:

1. Continuously update the TLS proxy software in order to fix any vulnerabilities. This includes the TLS proxy's cryptography libraries, such as OpenSSL or mbed TLS, which must be provided with the latest security updates.
2. The TLS should refuse to accept any incoming connections from the Internet, access to the management interface of the TLS proxy should restricted and the surrounding firewalls and access rights should be set restrictively.
3. The TLS proxy can be placed inside a separate network segment and monitored by an intrusion detection or prevention system and Security Information & Event Monitoring (SIEM).
4. The connection with the management interface should also be encrypted. You should use a unique certificate and secret key for this connection.
5. Do not unnecessarily store intercepted data traffic.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.