National Cyber Security Centre
Ministry of Justice and Security

TLS interception

Considerations and preconditions for the deployment of TLS interception

Factsheet FS-2017-05 | version 1.0 | 11 October 2017

TLS interception makes encrypted connections inside an organisation's network accessible for inspection. Deployment of this measure should be carefully considered in light of additional risks and should meet a number of important preconditions.

The reason for deploying TLS interception is that an ever-increasing number of internet services and internet connections is using encryption. This safeguards the integrity and confidentiality of the data transmitted and received. At the same time, however, this makes it more difficult for organisations to inspect internet traffic centrally in their network for malicious elements and for confidential organisational data that leaves the organisation via the Internet.

Background

Transport Layer Security interception (TLS interception) involves intercepting encrypted connections to make them accessible for inspection.[1] The intermediate stations that perform this activity are referred to as the 'TLS proxy' in this factsheet. 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. Organisations usually use TLS interception to detect and block malicious elements, such as viruses and malware, and data leakage within encrypted connections.[2]

Target audience

Chief Information Security Officers, privacy or data protection officers and information security officers.

The following parties have contributed to this factsheet:

Dutch Data Protection Authority (DPA), Dutch Tax and Customs Administration, National Communications Security Agency (NBV), Achmea, Equens Worldline, Rabobank and De Volksbank N.V.

[1] This obviously only concerns the interception of encrypted connections created in accordance with the TLS protocol.
[2] This is also known as Data Leakage Prevention (DLP).

The use of encrypted connections, for instance with Transport Layer Security (TLS) or its predecessor Secure Sockets Layer (SSL), is increasing. This safeguards the integrity and confidentiality of data transmitted by and received from internet services and provides certainty on the identity of the server. TLS therefore is an indispensable measure for providing internet services in a secure manner, such as webmail, internet banking and web shops. A disadvantage is that encrypted connections set up by malicious software, such as connections between malware and a command-and-control-server[3], can no longer be inspected due to the encryption. This hampers detection. A collateral development is that bona fide encrypted services offered by reputable cloud services are increasingly being misused for mala fide purposes, which impairs the effectiveness of exclusively blocking malicious IP addresses and URLs.[4]

TLS-proxies can be locally installed on endpoints, a method that is applied by some anti-virus scanners or firewalls. However, they are often deployed in central locations in an organisational network, such as the Internet connection. Although this factsheet focuses on the centrally organised variant, many of the risks and issues identified apply equally to the local versions. TLS proxies that handle incoming traffic for the organisation's servers (TLS reverse proxies) fall outside the scope of this factsheet.

Key facts

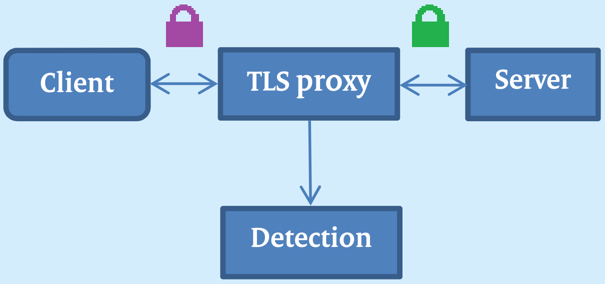
1. TLS interception entails that an organisation positions a TLS proxy between its own clients and a server in order to gain access to the content of the TLS connection.
2. Organisations usually apply TLS interception to the Internet connection to block inbound malware and prevent the leakage of confidential organisational data.
3. There are a number of important preconditions for implementing TLS interception in a secure and responsible manner, including a prior review of privacy aspects, correct configuration and the security of the TLS proxy and the controlled roll-out of certificates.
4. TLS interception should not be implemented separately but as an integral and carefully considered component of a broader set of measures for the implementation of information security policy.

How does TLS interception 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.



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?

Information security 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 received. The client software will subsequently only be able to

[3] Computers that are used to operate a botnet.
[4] Cyber Security Assessment Netherlands 2016, p. 44, see https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html.

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*.[5] Client authentication on the basis of a client certificate at the endpoint may also be difficult or 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.

Privacy risks

Before the organisation deploys TLS interception, it is appropriate to conduct a review of compliance with legal requirements. This should cover at least the processing of personal data, in view of the possible invasion of privacy.[8] More information on the legal framework for the processing of personal data is available on the Dutch Data Protection Authority's website.[9] [10] [11]

What does the NCSC recommend?

If, based partly on the review referred to in the previous section, you reach the conclusion that deployment of a TLS proxy is feasible and appropriate, you will need to gain a clear understanding of the technical requirements for the TLS proxy. A key aspect is that the TLS proxy sets up adequately secured connections with the client and the server. The description of the security characteristics of secure connections used in this factsheet is in line with those set out in the NCSC ICT security guidelines for Transport Layer Security (NCSC TLS guidelines).[12] The definitions and elaboration of **'sufficient'** and **'good'** settings are provided in the NCSC guidelines.

Tables 1 and 2, at the end of this factsheet, contain a number of basic technical requirements and best practices which can be used to determine whether the TLS proxy sets up secure connections. Table 1 relates to servers and Table 2 to clients. The basic requirements mentioned are, in accordance with the current state of the art, the minimum requirements a TLS proxy should meet in order to set up secure connections. The best practices serve as a guidance on the use of recent and additional security measures. An international survey has revealed that TLS proxies do not simply meet the basic requirements.[13] [14] It is important to obtain certainty on this aspect before selecting a product.

[5] Numerous mobile apps, such as internet banking apps, use certificate pinning.

[6] An example is the use of TLS 1.3, which is not yet supported by all TLS proxies. For more information, see https://www.security.nl/posting/505600/Google+stopt+TLS-update+Chrome+56+wegens+problemen

[7] Popular browsers such as Firefox and Chrome only support the EV certificates of specific Certificate Authorities. The TLS proxy cannot issue EV certificates, which means that the client cannot be provided with an EV certificate.

[8] It would also be advisable to consider whether there are any other legal impediments to the deployment of TLS interception.

[9] The website address is: https://www.autoriteitpersoonsgegevens.nl.

[10] For more information on the forthcoming EU General Data Protection Regulation, see https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving.

[11] For privacy information in the context of employee and employer, see: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/opinie-europese-privacytoezichthouders-over-privacyrechten-werknemers

[12] The TLS guidelines are available on: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html.

[13] Zakir Durumeric et al, ‘The security impact of HTTPS interception’, https://zakird.com/papers/https_interception.pdf.

[14] See also the warning issued by US-CERT: https://www.us-cert.gov/ncas/alerts/TA17-075A.

Exceptions based on risk management

Your organisation should make explicit choices on how it deals with setting up connections that are deemed insufficiently secure according to the current standards and this factsheet.[15] After all, the TLS proxy ultimately determines the certificate verification and the strength of the encrypted connection for all TLS connections intercepted by the proxy. As a general rule, the best way to proceed is to follow the NCSC TLS guidelines and the example of the modern browsers and to phase out insecure connection options at the same pace. Your organisation can make an exception to this rule based on a risk analysis, by weighing the desired level of compatibility against the risk for users and the organisation. You should limit exceptions to specific servers or domain names, whenever possible.

You should also consider the level of control and options individual users should have when setting up a connection that could be potentially insecure. For instance, will the user receive a notification and be able to click through to set up the connection nevertheless, or will a notification be issued to the user stating that the connection could not be set up due to the security policy? More control for individual users can help reduce the number of support requests from employees about connections that are not working, but it can at the same time increase the risks for the organisation. Feedback on errors to users is a point of attention. If a user sets up a TLS connection via a web browser, the necessary information can be provided to the user via the web browser. However, mobile apps often do not offer this option.

Finally, based on risk management you can decide to exclude parts of the organisational network from TLS interception. You could, for instance, opt to design a partitioned and isolated network segment without TLS interception for employees' private devices.[16] In addition, trusted destinations could also be excluded based on a domain name or IP address, or website categories.[17]

Forward secrecy and out-of-band detection solutions

The TLS proxy and the client exchange session keys for the encryption of the data to be transmitted (bulk encryption). There are two methods for exchanging keys: a traditional and a modern method. According to the traditional method, the client generates the session key and subsequently encrypts it with the public key of the TLS proxy. Using its secret key, the TLS proxy can decrypt the session key and use it for bulk encryption. This is the way in which RSA key exchange takes place. The secret key of the TLS proxy can be used to decrypt stored network traffic (including key exchange) at a later point in time. The modern method for determining the session key is based on the Diffie-Hellman protocol (DHE and ECDHE), where the session key is agreed by the TLS proxy and the client but is never transmitted over the network. Stored network traffic therefore does not contain the session keys, which means that it cannot be decrypted retroactively with the secret key of the TLS proxy (forward secrecy). For the combination of TLS proxy and an out-of-band[18] detection solution, this is a significant difference. If a session key has been transmitted, the detection solution can decrypt and inspect the encrypted traffic using the secret key of the TLS proxy. However, when using forward secrecy, the TLS proxy will need to provide the individual session keys or the complete unencrypted data stream to the detection solution to enable it to inspect the traffic.[19] For connection security reasons, the use of forward secrecy is preferred.

Safeguarding TLS proxy security

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. After all, 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. This implies that the TLS proxy as a rule refuses to accept any incoming connections from the Internet, access to the management interface of the TLS proxy is restricted and the surrounding firewalls and access rights should be set restrictively. In addition, 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). The connection with the management interface should also be encrypted. You

[15] For example public keys of insufficient length or a hash function for signing the fingerprint of the certificate of insufficient strength.
[16] An example is a Wi-Fi network separate from business systems that employees may use for private purposes.
[17] This is also referred to as 'whitelisting'.
[18] In this case the detection solution is not built into the TLS proxy.
[19] TLS version 1.3 will probably only support key exchange with forward secrecy. See https://www.ietf.org/mail-archive/web/tls/current/msg21278.html.

should use a unique certificate and secret key for this connection.[20] Furthermore, do not unnecessarily store intercepted data traffic. Lastly, you should 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. You should ensure that you purchase a support contract with your supplier and that you budget these costs for the future to avoid any unforeseen costs at a later stage.

TLS proxy implementation and integration

A TLS proxy and the associated detection solution will bring the greatest benefits if they are properly integrated within other security measures, such as Security Information & Event Monitoring (SIEM). More background information on this aspect can be found in the Guide to the implementation of detection solutions issued by the NCSC and the AIVD.[21] It is also worthwhile to consider choosing a different supplier for the signatures for the detection system that is linked to the TLS proxy, than the supplier of signatures for endpoint security systems, such as local virus scanners. In this way, any gaps in signature files are overcome as much as possible. Lastly, the TLS proxy should have sufficient capacity to process the datastreams. The required capacity can be determined on the basis of the maximum connection speed of the internet connection or on the basis of historical data on usage of the internet connection. From a future-proofness perspective, it would be advisable to factor in a certain margin given that internet connections are becoming faster, the volume of traffic is growing and an ever-increasing number of internet services is using TLS.[22] During the first few weeks of actual implementation, you should ensure that sufficient support capacity is available to troubleshoot any unforeseen problems.

Perspective for action

- Before deploying TLS interception, conduct a review of compliance with legal requirements, covering at least the processing of personal data.
- Deploy TLS interception selectively and not unnecessarily.
- Test the TLS proxy against the information security requirements specified and configure it in accordance with this advice.
- Verify that the TLS proxy supplier will supply updates within a short time frame when vulnerabilities in the TLS proxy are identified.
- Protect the TLS proxy itself against attacks.
- Integrate the TLS proxy within the wider set of other security measures.
- Ensure sufficient support capacity to troubleshoot any unforeseen problems occurring after implementation.

In conclusion

On the one hand, TLS interception can enhance the information security of an organisation by enabling detection of malicious elements or confidential organisational data that is transmitted via TLS connections. On the other hand, it poses risks to information security and privacy. It is advisable to regard TLS interception not as low-hanging fruit, but rather as a measure that can supplement the broader array of security measures already in place. You should carefully weigh the usefulness and necessity in the context of other security measures and deploy TLS interception selectively. Conduct a prior review of compliance with legal requirements, covering at least the processing of personal data. Invest sufficient time and effort into clearly identifying and fulfilling information security related and other preconditions.

[20] This is because there is a risk that the same certificate and secret key are being used by other instances of the TLS proxy. In such a case, an attacker can extract the certificate and the secret key from that other instance and subsequently misuse it to intercept connections with the management interface of your TLS proxy.

[21] The guide is available on: https://www.ncsc.nl/actueel/whitepapers/handreiking-voor-implementatie-van-detectie-oplossingen.html.

[22] For the statistics, see: https://www.google.com/transparencyreport/https/metrics/?hl=en.

Table 1 Technical requirements for TLS proxies in order to set up secure connections to servers

Basic requirements

- The TLS proxy prefers the latest version of TLS for setting up connections.[23]
- The TLS proxy prefers the use of forward secrecy for setting up encrypted connections.
- The TLS proxy supports cipher suites, the strength of which is **good** or **sufficient**, and follows the server's preference for setting up a connection.
- TLS renegotiation and TLS compression are configured in accordance with the NCSC TLS guidelines.
- The TLS proxy validates server certificates at least for the following[24]:
  a. the validity of the server certificate for the domain requested (Subject Alternative Name and Common Name);[25]
  b. the validity period of the server certificate;
  c. the status of the server certificate based on CRL or OCSP;[26]
  d. the validity of the certificate chain, where the server certificate has been signed with a trusted root certificate (root CA) or an intermediate certificate (intermediate CA);
  e. the certificate restrictions, as indicated in attributes. Examples are whether the certificate is permitted to be used as a server certificate or whether the length of the chain of certificates does not exceed the permissible length of one of the root or intermediate certificates.[27]
  f. the strength of the hash function used for signature of the fingerprint, the strength of which must be **good**.[28]
- The length of the public key (RSA or ECDSA) of the certificate should be **sufficient** or **good.**

You can use a website such as badssl.com to test in practice whether the TLS proxy actually performs the necessary validations and which cipher suites are supported.

Best practices

- HTTP Strict Transport Security (HSTS) headers are respected and forwarded to the client.
- The TLS proxy supports the latest certificate verification techniques at the same pace as modern browsers:
  a. certificate verification using HTTP Public Key Pinning (HPKP);[29]
  b. certificate verification using DANE and TLSA.[30]
- The standard trust list of the TLS proxy for root and intermediate certificates matches that of modern web browsers, such as Mozilla Firefox. The list is updated regularly.[31]

[23] TLS version 1.2 at the time of writing this factsheet.

[24] The server certificate is the certificate of the server with which the TLS proxy makes a connection, such as a website. If validation errors occur, the TLS proxy should cut off the connection with the server and no longer forward the client's request to the server.

[25] See RFC 2818. If a Subject Alternative Name exists, it must be used for validation purposes. If it does not exist, the Common Name will be used for validation purposes.

[26] Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) enable a certificate to be checked to determine whether it has been revoked.

[27] This involves checking the attributes of the certificate in accordance with RFC 5280 of the X.509 specifications, such as the *basic constraints*. This indicates within which limits a certificate is permitted to be used. Consider for what purposes a certificate is permitted to be used, such as a server certificate, the signing of software, signing as CA, etc. Also consider the maximum length of the chain of certificates.

[28] Modern browsers are phasing out support for SHA-1 certificate signature as it is now deemed insecure. It would be advisable to follow suit.

[29] The TLS proxy will be able to support HPKP only for the internet server. HPKP verification by the client is no longer possible with TLS interception. Depending on the client software, the HPKP header will need to be deleted by the TLS proxy.

[30] This requires that the TLS proxy also supports and validates DNSSEC.

[31] This list is available on: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/.

Table 2 Technical requirements for a TLS proxy in order to set up secure connections to clients

Basic requirements

- If the connection between the TLS proxy and the server runs via TLS, the connection between the TLS proxy and the client should also run via TLS.
- Do not use the standard root certificate (root CA) that is supplied with the TLS proxy, because the corresponding secret key can easily be retrieved by third parties. This will enable them to carry out a man-in-the-middle attack on any client who trusts the certificate. You should therefore generate a new unique private key and a certificate. Store the private key in a secure location.[32] Do not use the private key for other proxies.
- For interception purposes, do not use an intermediate certificate from a supplier which, by default, is trusted by browsers.[33]
- Ensure a careful procedure for installing the root certificate (root CA) on clients to ensure that they trust the TLS proxy. This will avoid users from growing accustomed to clicking through certificate errors to make a connection, with all the associated risks.
- Personal client certificates for outgoing connections, installed on the TLS proxy, may only be used by authorised users.
- The TLS proxy supports and prefers cryptographic algorithms of **good** or **sufficient** strength for setting up connections with clients concerning:
  a. Certificate verification
  b. Key exchange
  c. Bulk encryption, including operating mode
  d. Hashing
- The length of the public key (RSA or ECDSA) of the certificate is **sufficient** or **good.**
- The strength of the hash function used for the signature of the fingerprint of the certificate is **good.**[34]
- The certificate used for interception contains the Subject Alternative Names laid down in the internet server's original certificate.
- TLS renegotiation and TLS compression are configured in accordance with the NCSC TLS guidelines.

Best practices

- The certificate used for interception contains the details of the organisation as laid down in the internet server's original certificate.
- Use an existing PKI environment within the organisation to roll out the root certificate for clients.
- The TLS proxy prefers the use of forward secrecy for setting up encrypted connections with the client.

[32] A Hardware Security Module (HSM) can, for instance, be used for this purpose.

[33] The use of these unlimited intermediate certificates, which can be used for any domain, is unauthorised according to the CA/B Forum Baseline Requirements. If such a certificate appears outside of your internal network, it constitutes a risk for the information security of other organisations and users. The browser manufacturers will most likely block this particular intermediate certificate, which means that the TLS proxy will suddenly become inoperative.

[34] Modern browsers are phasing out support for the SHA-1 for certificate signature as it is now deemed insecure. It would be advisable to follow suit.

Publication
National Cyber Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (70) 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2017-05 | version 1.0 | 11 October 2017

This information is not legally binding.