Network
+ Security
+ Cloud

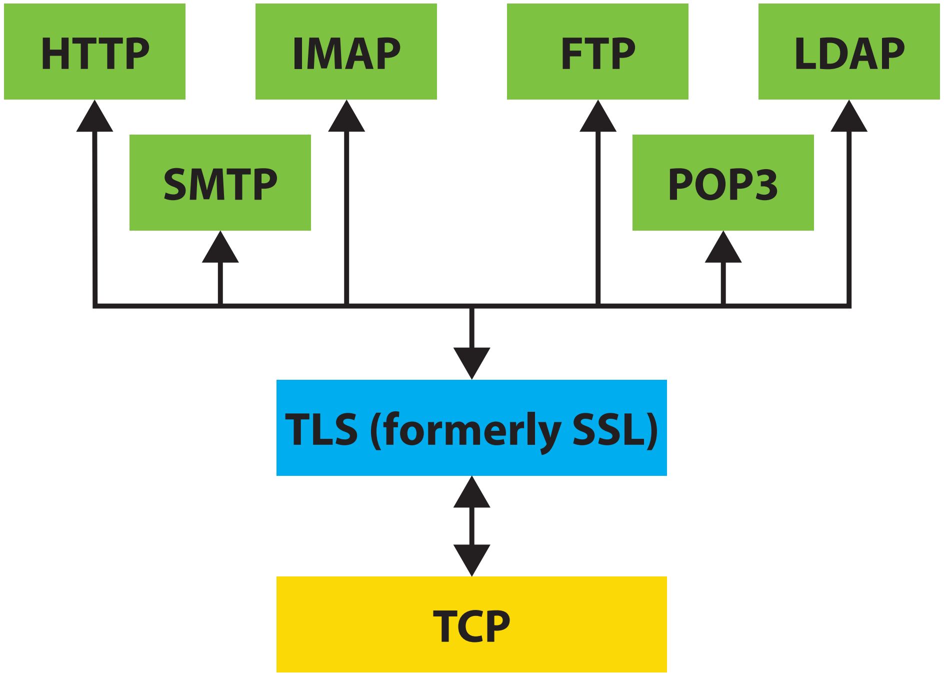
A TECHNOLOGY BRIEF ON SSL/TLS TRAFFIC

TECHNOLOGY PRIMER

This document provides an overview of SSL/TLS technology and offers examples of how Blue Coat solutions can help manage the increasing SSL traffic within enterprise networks and protect them from growing hidden threats and advanced malware.

What is SSL/TLS?

Regardless from where you access your cloud, mobile or web-based applications, the connection between your device and any other point can be routed through dozens of independent network systems. Through snooping, spoofing, and other forms of Internet eavesdropping, unauthorized individuals can identify and steal personal data and other confidential information such as credit card numbers, customer and partner information and PIN numbers.



HTTP + SSL/TLS + TCP = HTTPS

Figure 1 – SSL/TLS Enables Secure, Authenticated Communications

The Secure Sockets Layer (SSL) protocol was developed to transfer information privately and securely across the Internet. SSL is layered beneath application protocols such as HTTP, SMTP, POP3, and FTP and above the connection protocol TCP/IP. It is used by the HTTPS access method. Without SSL, the only security provided is authentication of the client by the server via a username and password. Communications between the client and the server is in the open and not secure. Figure 1 illustrates the difference between a non-secure HTTP request and a secure SSL request.

While Transport Layer Security (TLS) is the successor of the Secure Sockets Layer (SSL) protocol and the dominant industry standard; they are both cryptographic protocols that provide secure communications on the Internet for such things as web browsing, cloud access, e-mail communications, instant messaging and other data transfers. There are slight functionality differences between SSL and TLS and, SSL is, knowingly, less secure than the current TLS, but the protocols remain substantially the same. Due to these numerous vulnerabilities in SSL, Blue Coat provides retroactive support for SSL, but strongly recommends all customers migrate their websites and servers to supporting connections over TLS1.1 or 1.2. For purposes of simplicity and based on familiarity, we'll use the term 'SSL' throughout this document when referring to these collective standards.

The benefit of SSL is secure, authenticated communication over public or private networks. The growing disadvantage of SSL is that it introduces 'blind spots' within the network infrastructure due to its fundamental objective of securing communications. As the content and data within SSL traffic remains hidden to most network security tools, the risk of data breaches, exfiltration and theft is higher. Traditional and even modern network security devices like Next Gen Firewalls (NGFW), Intrusion Prevention Systems (IPS), Data Loss Prevention (DLP) and anti-malware/sandbox solutions are ineffective at identifying and blocking advanced treats that use SSL to hide.

Who Uses SSL/TLS?

As SSL is the de facto standard for encrypted and authenticated communications between clients and servers on the Internet, it is pervasive in enterprise networks across the world. Current estimates indicate that 50% or more of enterprise network traffic is SSL-based and growing rapidly. Virtually all online purchases, cloud-based transactions and browser-based monetary transactions that occur on the Internet are secured by SSL. However, SSL is not just limited to securing web browsing and e-commerce transactions. Its use goes beyond HTTPS / Web / Port 443 traffic as per the following examples:

- Email protocols such as SMTP, IMAP, POP3 running over TLS
- Secure file transfer using FTP over TLS
- Protocols such as SPDY running over TLS - used by Google and Facebook
- Application-specific protocols running over SSL such as legacy transaction protocols
- Machine-to-machine applications such as credit card authorization running over SSL
- Proprietary protocols on top of SSL or TLS which may be legitimate application traffic or could be protocols being used by malware

How Does SSL/TLS Work?

When a client and server communicate, SSL ensures that the connection is private and secure by providing authentication, encryption, and integrity checks. Authentication confirms that the server, and optionally the client, is who they say they are. Encryption using a unique session key securely negotiated between client and server creates a secure "tunnel" between the two that prevents any unauthorized system from reading the data. Integrity checks guarantee that any unauthorized system cannot modify the encrypted stream without being detected.

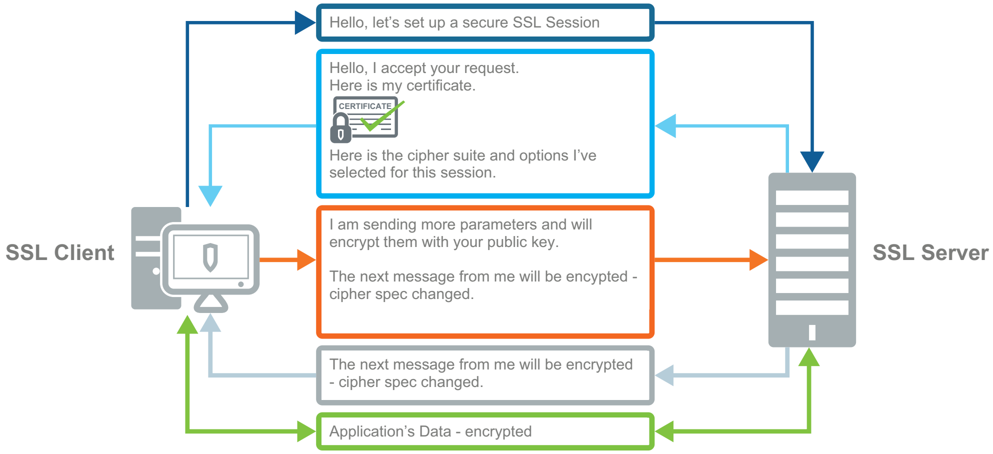
SSL-enabled devices – such as clients using web browsers like MozillaTM, SafariTM or ChromeTM - and SSL-enabled servers (such as Apache or Microsoft IISTM) confirm each other's identities using digital certificates. Digital certificates are issued by trusted third parties called Certificate Authorities (CAs) and provide information about an individual's claimed identity, as well as their public key. Public keys are a component of public-key cryptographic systems. The sender of a message uses a public key to encrypt data. The recipient of the message can only decrypt the data with the corresponding private key. Public keys are known to everybody; private keys are secret and only known to the owner of the certificate. By validating the CA digital signature on the certificates, both parties can ensure that an imposter has not intercepted the transmission and provided a false public key for which they have the correct private key. SSL uses both public-key and symmetric key encryption. Symmetric key encryption is much faster than public-key encryption, but public-key encryption provides better authentication techniques. So SSL uses public key cryptography for authentication and for exchanging the symmetric keys that are used later for bulk data encryption.

The secure tunnel that SSL creates is an encrypted connection that ensures that all information sent between an SSL-enabled client and an SSL-enabled server remains private. SSL also provides a mechanism for detecting if someone has altered the data in transit. This is done with the help of message integrity checks. These message integrity checks ensure that the connection is reliable. If, at any point during a transmission, SSL detects that a connection is not secure, it terminates the connection and the client and server establish a new secure connection.

SSL/TLS Transactions

The SSL transaction has two phases: the SSL Handshake (the key exchange) and the SSL data transfer. These phases work together to secure an SSL transaction.

Though the authentication and encryption process may seem rather involved, it happens in less than a second. Generally, the user does not even know it is taking place. However, the user is able to tell when the secure tunnel has been established since most SSL-enabled web browsers display a small closed lock 🔒 at the bottom (or top) of their screen when the connection is secure. Users can also identify secure websites by looking at the website address; a secure website's address begins with **https** rather than the usual **http**.



Hello, let's set up a secure SSL Session

Hello, I accept your request.
Here is my certificate.

Here is the cipher suite and options I've selected for this session.

I am sending more parameters and will encrypt them with your public key.

The next message from me will be encypted - cipher spec changed.

The next message from me will be encrypted - cipher spec changed.

Application's Data - encrypted

Figure 2 – Illustrates the Sequence of SSL transactions

Cipher Suites and SSL/TLS

SSL supports a variety of different cryptographic algorithms, or ciphers, that it uses for authentication, transmission of certificates, and establishing session keys. SSL-enabled devices can be configured to support different sets of ciphers, called cipher suites. If an SSL-enabled client and an SSL-enabled server support multiple cipher suites, the client and server negotiate which cipher suites they use to provide the strongest possible security supported by both parties. A cipher suite specifies and controls the various cryptographic algorithms used during the SSL handshake and the data transfer phases. Specifically, a cipher suite provides the following:

- **Key exchange algorithm:** The asymmetric key algorithm used to exchange the symmetric key. RSA, Diffie-Hellman (DHE) and Elliptic Curve Diffie-Hellman (ECDHE) are common examples.
- **Public key algorithm:** The asymmetric key algorithm used for authentication. This decides the type of certificates used. RSA and DSA are common examples.
- **Bulk encryption algorithm:** The symmetric algorithm used for encrypting data. RC4, AES, DES, 3DES and Camellia are common examples.
- **Message digest algorithm:** The algorithm used to perform message integrity checks and authentication. SHA and SHA256 are common examples.

The cipher suites illustrated below provide 2 examples of modern cipher suites used within SSL/TLS.

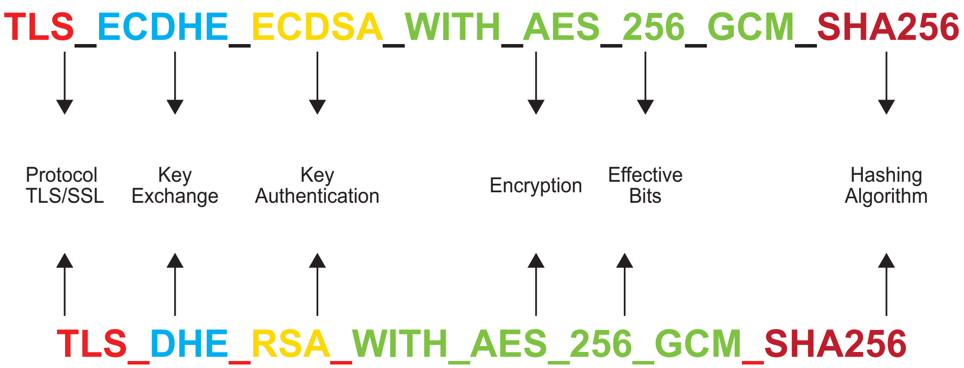


Figure 3 – Cipher Suite Examples

Perfect Forward Secrecy

While all of the above attributes of a cipher suite are relevant and necessary, some of the underlying protocols and standards have become obsolete in recent years due to on the ongoing evolution of stronger, more secure cryptography. More specifically, key exchange mechanisms have evolved in support of Perfect Forward Secrecy (PFS) – which is a method to ensure that obtaining a copy of a server private key does not allow decryption of previously captured encrypted flows to that server. PFS mechanisms generate the session key in such a way that it cannot be derived by looking at a captured encrypted flow even if the server's private key is available. Non PFS mechanisms allow the session key to be derived if the server's private key is available. PFS means that even if a server's private key is acquired it is impossible to decrypt any previously captured SSL sessions to that server or any new SSL sessions to the server.

Standards that support PFS for key exchange include Diffie-Hellman (DHE) and Elliptic Curve Diffie-Hellman Exchange (ECDHE) – which are meant to replace replay-vulnerable, and, thus, less secure, standards like RSA for key exchange. Most, if not, all information providers, service providers and application developers or providers offer support for PFS in their cryptography suites today.

Understanding PKI and Certificate Authorities

In public key infrastructure (PKI) cryptography, an entity that issues digital certificates is known as a Certificate Authority (CA). A digital certificate verifies the ownership of a public key by the named subject of the certificate. This allows others devices and systems to rely upon signatures for secure, authenticated communications. A Certificate Authority is a trusted third-party - trusted both by the owner of the certificate (e.g. a server) and by the party relying upon the certificate (e.g. a client or another server).

Regarding SSL communications, trusted digital certificates are typically used to make secure connections between devices. Trusted certificates are required to eliminate any opportunity by a malicious party pretending to be a valid target (i.e. server or client) of intercepting the communications. Such a scenario is commonly referred to as a man-in-the-middle (MITM) attack.

The client uses the CA certificate to verify the CA signature on the server certificate, as part of the checks before establishing a secure connection. Usually, client software such as web browsers includes a set of trusted CA certificates. Likewise, network and security devices that utilize SSL certificates include and require a set of trusted CA certificates for protected communications.

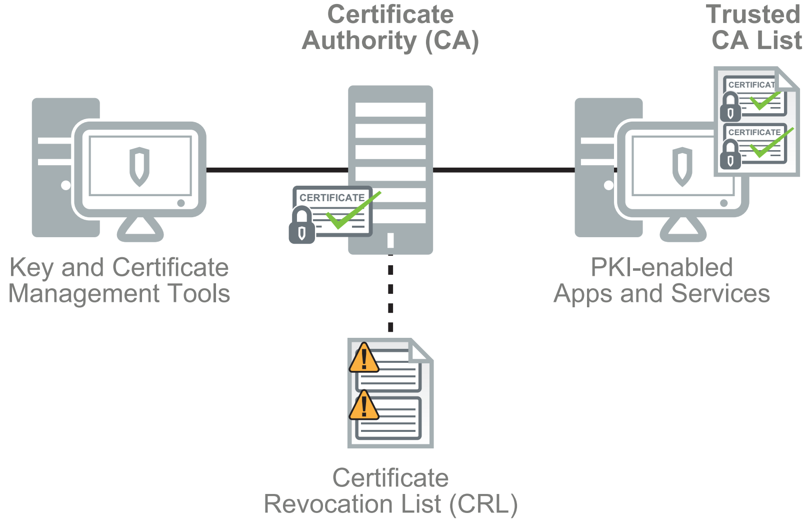

Certificate Authority (CA)
Trusted CA List
CERTIFICATE
CERTIFICATE
CERTIFICATE
Key and Certificate Management Tools
PKI-enabled Apps and Services
Certificate Revocation List (CRL)

Figure 4 – PKI and Its Components

A root CA certificate may be the origin and basis to issue multiple intermediate CA certificates with varying validation requirements. Most organizations today rely on a varying combination of root and intermediate CA servers to ensure secure communications.

Man-in-the-Middle

As referenced earlier, Man-in-the-Middle (MITM) attacks are a big concern in organizations across the globe. Certificate Authorities and their supporting digital certificates and signatures provide a means to eliminate threats posted by MITM attacks, but there is more to address than just implementing CAs in pursuing a stronger network defense posture.

To recap, a MITM attack is an attack where an intruder secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. These attacks can be used against many cryptographic protocols, in which the intruder must be able to intercept all relevant messages passing between the two devices and inject new ones. A common scenario for a MITM attack includes a hacker inserting himself in unencrypted W-Fi communications in public locations such as cafes and airports.

MITM uses aren't always nefarious. In the case of inspecting and analyzing traffic for advanced malware and potential threats, a MITM process is implemented in common network security solutions like web proxies and network visibility technologies to identify and mitigate threats. (See Figure 5)

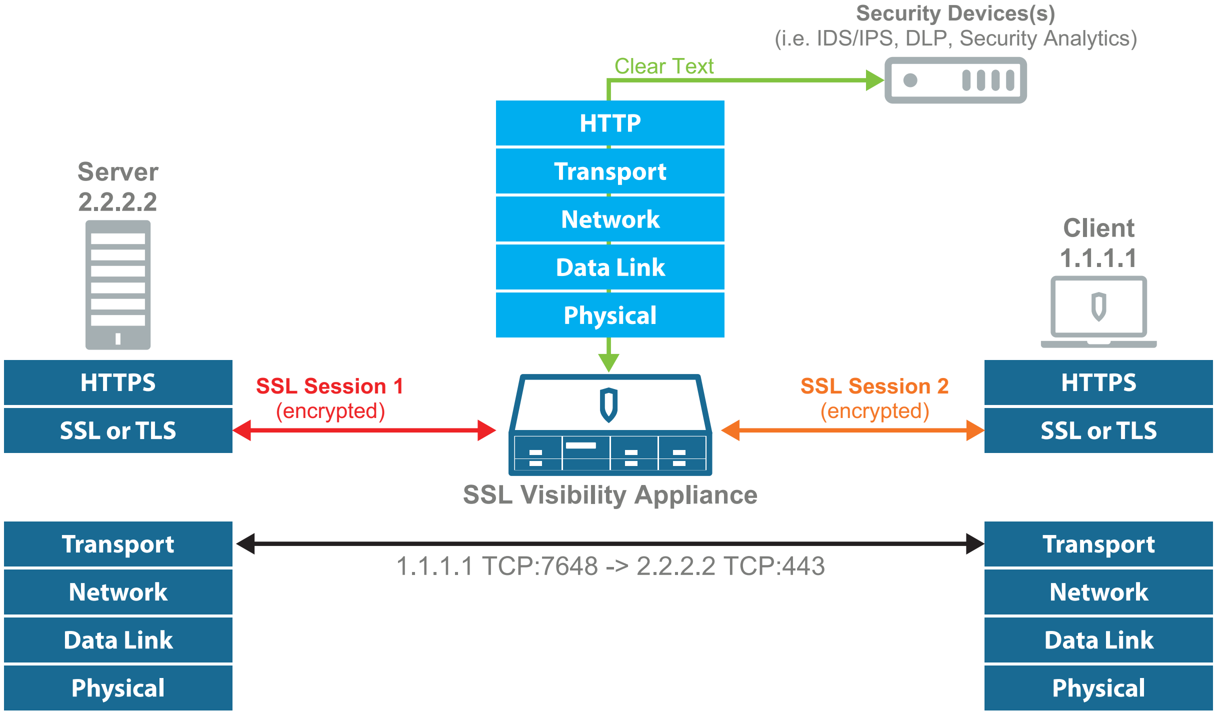


Figure 5 – The SSL Visibility Appliance and Man-in-the-Middle (MITM)

Regarding SSL communications, mechanisms are in place to prevent MITM attacks by including end point / device authentication using mutually trusted CAs.

Vulnerabilities

Cyber-attacks can also be based on known or unknown vulnerabilities within the cryptography standards themselves. Case-in-point is the Heartbleed vulnerability which came to fruition in the spring of 2014 and highlighted a weakness in the open-source OpenSSL code used by many web servers, network and security devices worldwide. Due to a lack of checking between the data size field and the actual data within an SSL packet, cybercriminals could potentially gain access to passwords and digital certificates that subsequently lead to more information loss. One way to mitigate this vulnerability until clients or servers can be patched is to insert a legitimate MITM device to detect the Heartbleed exploit and prevent the SSL/TLS session from taking place.

Solutions for Managing SSL/TLS Traffic

Blue Coat's Encrypted Traffic Management solutions provide the most cost effective means to eliminate the encrypted traffic blind spot while preserving privacy, policy compliance, and the investment in the security infrastructure.

As a key component of this solution set, the SSL Visibility Appliance is a high capacity SSL inspection, decryption and management appliance, scaling to 9 Gbps of SSL decryption and is capable of feeding decrypted information to multiple security tools simultaneously. The SSL inspection and decryption capabilities provided by the SSL Visibility Appliance enable existing security and network appliances such as IDS/IPS, DLP, Malware Analysis, NGFW and forensics or security analytics platforms to access the plaintext within SSL flows, thereby enabling the security appliance to effectively do its job, even with SSL encrypted traffic. Unmodified applications running on devices attached to the SSL Visibility Appliance gain visibility into the content of the SSL traffic. SSL inspection is a complex and computationally intensive process that can easily become a performance bottleneck unless implemented with appropriate hardware acceleration techniques.

From a deployment standard, this product is a *fully transparent proxy* – meaning it does not allow modification of the security profile (cipher suite) or encrypted data of an SSL flow. As a "bump-in-the-wire" device, the appliance needs to be placed in line. The Ethernet ports that are used to connect it to the data network do not have IP addresses, and the clients and servers continue to communicate with each other's IP addresses even while the SSL Visibility is active. Unlike non-transparent proxies, the SSL Visibility Appliance can, therefore, be used to process traffic flowing within an IP subnet. It can also handle traffic between subnets. (See Figure 6)

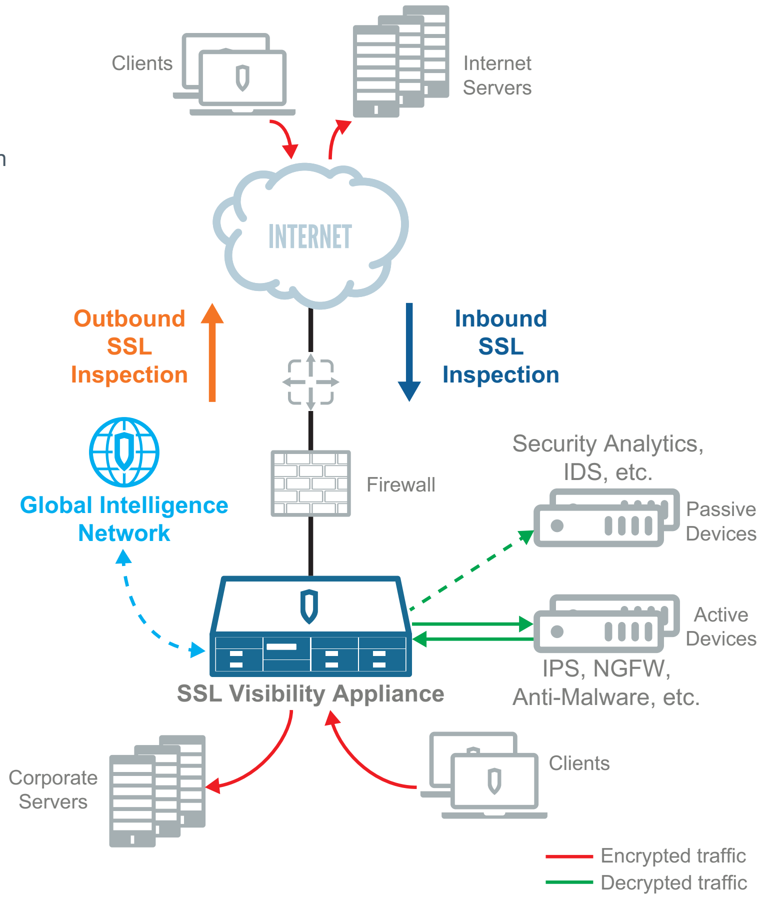


Figure 6 – Deploying the SSL Visibility Appliance

The main function of the SSL Visibility Appliance is to decrypt SSL traffic to obtain the plaintext sent within the SSL-encrypted session. The plaintext information is fed to an attached device such as an IDS/IPS or forensics appliance for processing or analysis. The plaintext data stream is repackaged as a valid TCP stream, so unmodified applications that are hosted on the attached device can process the received plaintext stream as if it was never encrypted.

Lastly, the SSL Visibility Appliance serves as an effective policy enforcement point to control SSL/TLS traffic throughout the enterprise, reducing risks posed by encrypted traffic, while maintaining compliance with relevant privacy policies and regulatory requirements. Utilizing its unique 'Host Categorization' service for policies, organizations can easily create and customize granular policies to selectively decrypt traffic to meet their business needs (e.g. "do not decrypt financial or banking traffic"). Furthermore, policies can easily be set to control obsolete or weak ciphers and standards – such as traffic using the SSL v3.0 or MD5 standards. This enables organizations to effectively balance security with data privacy and compliance requirements. These policies also utilize Blue Coat's market-leading Global Intelligence Network to exchange and update Host Categorization data, as well as threat and malware knowledge worldwide.

PKI and the SSL Visibility Appliance

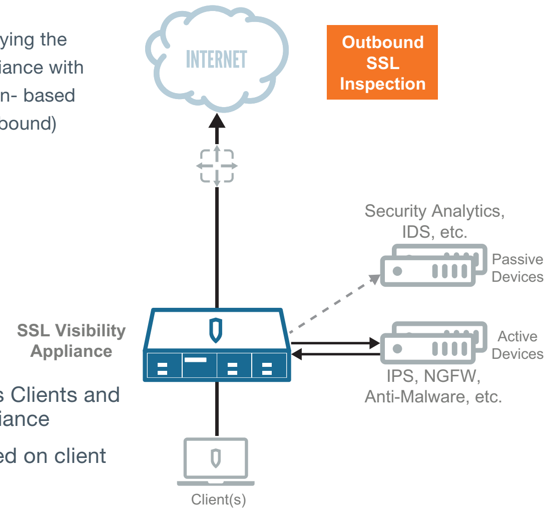
When deploying the SSL Visibility Appliance, a trust relationship has to be established between the clients, servers and the appliance itself in order to ensure secure communications. The SSL Visibility Appliance is emulating server certificates in real-time and these emulated server certificates are signed by a trusted CA installed in the SSL Appliance.

SSL Visibility Appliances and CAs

There are two primary mechanisms that can be used in order to inspect SSL traffic depending on what certificate and key information is available and how the inspection device is deployed in the network.

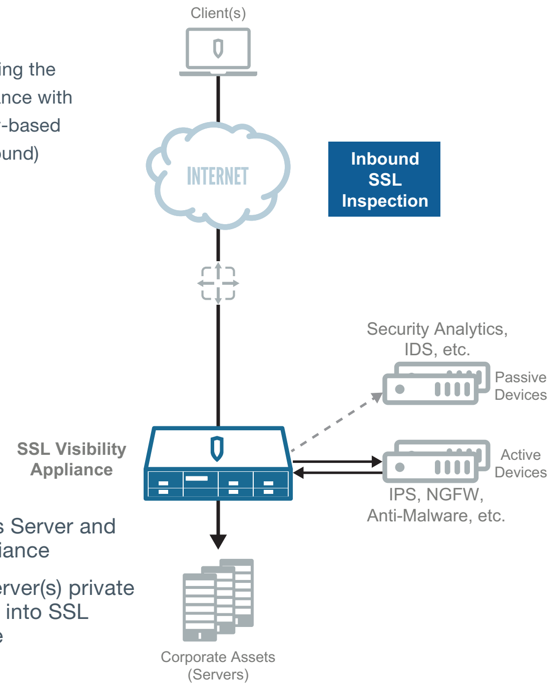
1. Certificate Re-Signing is the method used to inspect SSL/TLS to external servers for which the organization does not have access to the servers' certs and private keys. (See Figure 7)
   - **Certificate Re-sign based Inspection** – relies on the inspecting device having a trusted CA certificate that can be used to sign SSL server certificates that have been intercepted and modified. This inspection method is used for outbound communications leaving an enterprise and destined for an external SSL server. The CA certificate used by the SSL Visibility Appliance can be self-signed, generated on box and then signed by an enterprise CA that processes the Certificate Signing Request (CSR) from the SSL appliance, or generated by an enterprise CA and loaded onto the appliance.
   - **Self-Signed Server Certificates** – the SSL Visibility Appliance can use certificate re-sign to process self-signed server certificates or can simply replace the keys in the self-signed server certificate in which case the CA in the SSL appliance is not used and the server certificate remains self-signed.
2. Known Server Key (KSK) – relies on the SSL Visibility Appliance having a copy of the servers' private keys and certificates and is used for inbound communications entering an organization destined for an internal SSL server. Certificates and keys can easily and securely be imported into the SSL Visibility Appliance via the management interface or by using a third-party Enterprise Key and Certificate Management (EKCM) solution such as Venafi's Trust Protection Platform to provision the keys and certificates into the SSL Visibility Appliance. (See Figure 8)

Figure 7 – Deploying the SSL Visibility Appliance with Certificate Re-sign- based Inspection (outbound)



- Enterprise controls Clients and SSL Visibility Appliance
- Install CA as trusted on client machines

Figure 8 – Deploying the SSL Visibility Appliance with Known Server Key-based Inspection (inbound)



- Enterprise controls Server and SSL Visibility Appliance
- Install copies of server(s) private key and certificate into SSL Visibility Appliance

Next Steps: Preparing for Encrypted Traffic Management

As IT Security teams start planning and preparing to deploy a solution for managing SSL/TLS traffic, it's extremely important to consider several key factors in making this transition as smooth and non-disruptive as possible. Review the following for additional guidance:

KNOWLEDGE AND SKILLS TRAINING	**The IT Network and Security teams should be familiar with the technologies, skills and processes surrounding SSL/TLS and SSL/TLS management.**
PKI knowledge	• Understanding certificates, certificate authorities, keys, key management is paramount to your success.
Cipher Suite / Cryptography Knowledge	• Understanding industry standards, cipher suites, key exchange mechanisms and more is essential for a solid defense-in-depth security posture. • Also realize that ciphers continuously evolve while others become obsolete. Case in point, the SSL v3.0 standard, RC4 streaming cipher and the SHA (SHA-1) hash algorithm are obsolete –or about to become obsolete – and your IT security infrastructure should upgrade any systems utilizing these weak and outdated standards.
ADDITIONAL IT ASSETS AND PROCESSES	**New technologies, products and/or services may be required in your organization for a successful encrypted traffic management deployment.**
Key and Certificate Management and Storage	• Your organization will need the means to effectively manage keys and certificates (i.e. add, revoke, etc.). While certs and keys can be imported and added via most network and security tools that pass SSL/TLS traffic, a more efficient, centralized management approach may prove easier for you. Enterprise Key and Certificate Management (EKCM) solutions by companies like Venafi, as well as Hardware Security Module (HSM) solutions by companies like Gemalto (formerly SafeNet) can address your needs.
CROSS-ORGANIZATION COLLABORATION	**Managing encrypted traffic is not just an IT security issue, but one that involves multiple teams across an organization.**
Legal / Compliance / Risk Management Teams	• Meet with your Legal, Compliance or Risk Management teams to discuss what legislative compliance mandates must be met. If you're a multi-national organization, this is broader than just addressing local, state and US federal policies, so your team should plan accordingly. Ensuring Data Privacy is the key concern
Human Resources (HR)	• As your HR team establishes the corporate policies and acceptable behavior for your organization and its employees, discussing these policies and how they translate into rule sets, scripts or polices in your network security infrastructure is important. Besides establishing communication norms regarding personal email and social media use at work, cultural considerations and data privacy issues are also relevant here.

BLUE COAT®

Network
+ Security
+ Cloud

Conclusion

SSL/TLS has become the universal standard for authenticating and encrypting communications between clients and servers. It is pervasive in today's enterprises and growing rapidly due to the rapid increase in cloud, mobile and web applications. However, SSL poses a security threat by introducing a "blind spot" which increases the risk of advanced malware penetrating an organization and possibly exfiltrating proprietary data, without detection.

Blue Coat Systems provides its unique Encrypted Traffic Management solutions to resolve this dilemma and enable organizations to inspect, decrypt and manage SSL traffic to eliminate this dangerous "blind spot", enhance the existing security infrastructure with new and complete visibility in to all network traffic and preserve data privacy to maintain compliance.

For more information and assistance in managing your encrypted traffic, check out Blue Coat's website: www.bluecoat.com/uncoverssl

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000