Security: In An Encrypted World

EFFICIENT SECURITY THROUGH COMPLETE NETWORK VISIBILITY

Encryption is one of the basic enabling technologies of the Internet. We rely on it to do business with partners, shop online, send email, and access applications while maintaining our privacy, identities, and security. It is so important that most cloud providers, such as Google, Facebook, and others, along with most mobile apps, have already switched to using encryption by default on all connections. In fact, as of 2016, both Mozilla[1] and Google[2] have shown that over 50% of sites visited via their browsers use encryption. **Moreover, By 2019, Gartner believes more than 80 percent of enterprise Web traffic will be encrypted**. The widespread use of Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) encryption, which are both commonly referred to as “SSL,” has undoubtedly contributed to the rapid growth of the Internet as a revolutionary conduit for business.

As SSL/TLS encryption has become more important, encryption standards have changed over time to address security weaknesses or stay ahead of faster computers that make brute-force attacks easier. One such recent update is the introduction of ephemeral key cryptography, which makes encryption more secure and encourages even more widespread adoption.

[1] https://letsencrypt.org/stats/

[2] https://www.google.com/transparencyreport/https/metrics/?hl=en

TLS/SSL IS NOT RISK FREE

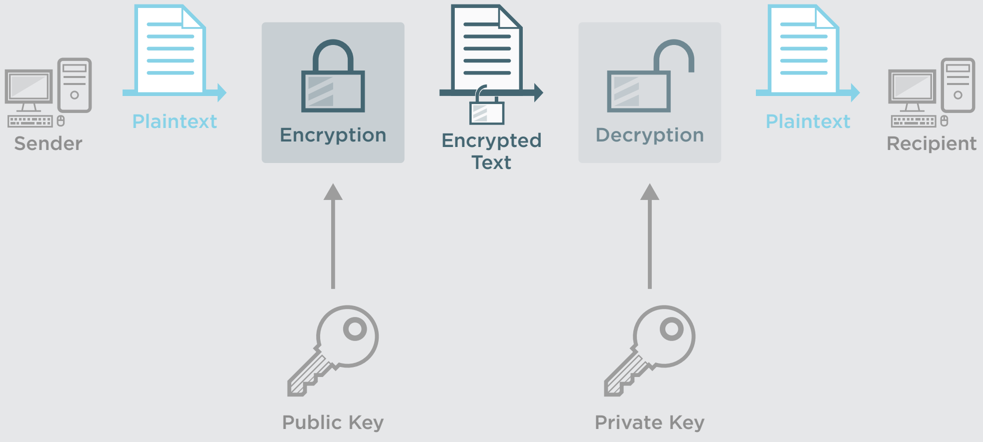
Complete Security Requires Complete Visibility

As useful as the widespread use of encryption is in improving the security of data in transit, it also poses new challenges to enterprise information technology (IT) and security operations: malicious traffic is increasingly encrypted along with good traffic. Gartner estimates that, by 2017, more than 50% of network attacks will use SSL/TLS[3]. Malware downloads are a common example of malicious traffic that is obscured by encryption; a user may click on a phishing link or otherwise visit a malicious website over SSL, and the website, in turn, pushes malware down to the client over the encrypted session. Similarly, most popular Web mail services rely on SSL for privacy, but a malicious attachment in an e-mail would be downloaded onto the user's system over that encrypted link. Bad things happen in blind spots, and encryption can create a significant blind spot for security administrators

The challenge for IT and security operations professionals is how to balance the need for data protection and security. Complete security requires complete visibility, in order to avoid blind spots and subject all traffic to default inspection. Especially with the adoption of ephemeral key encryption, the best (and, indeed, only) way to inspect encrypted traffic on the network is via the use of an active SSL proxy.

EPHEMERAL KEY CRYPTOGRAPHY

When data is encrypted for transmission over a computer network, it is scrambled or "coded" for protection. As in the diagram below, the technology basically works by exchanging information that is coded via a public key (provided by the server) and sent over the internet. The receiving party (server) is able to un-code, because it has the other half of the equation, the private key.

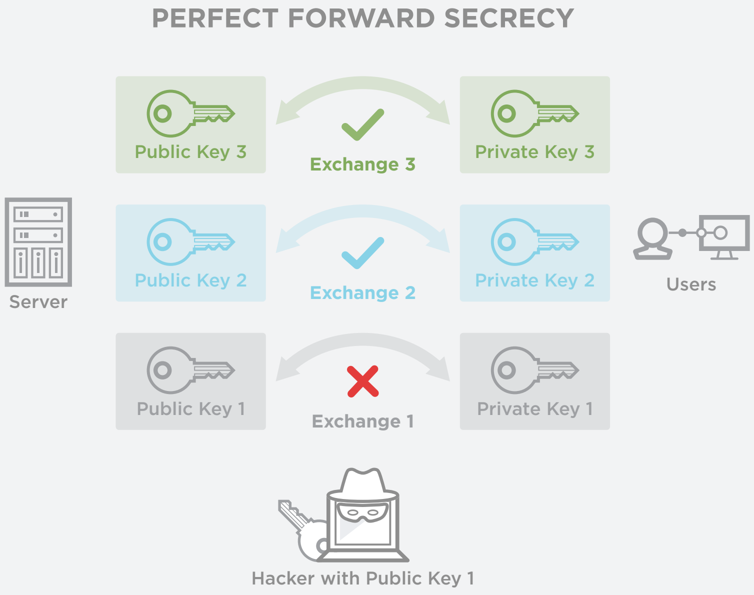


[3] D'Hoinne, Jeremy and Hills, Adam. Gartner. Security Leaders Must Address Threats from Rising SSL Traffic, December 9, 2013. Gartner RAS Core Research Note: G00258176

The dominant encryption technology had been RSA, which uses static keys. This means that a server has a given key for its communications, and any observer who has a copy of that key can decrypt any traffic to that server. This was convenient for many uses: for troubleshooting or forensics, encrypted data could be streamed directly to disk and decrypted on-demand later, if needed. Maintaining an independent audit trail of e-commerce transactions was relatively straightforward, as a "passive" SSL decryption device or application could simply observe a connection passively and decrypt it so long as it had a copy of the server's private key.

This convenience, of course, has a downside. If the private key used by, for example, a popular online bank is somehow compromised, a hacker could sit on a public Wi-Fi network and easily decrypt any sessions with that bank via the same passive decryption technique. This obviously poses a significant risk to online privacy and security. To address this risk, many organizations and regulatory bodies are shifting to using and mandating ephemeral key encryption, most commonly Elliptic curve Diffie–Hellman Ephemeral (ECDHE), in which a new key is generated for each exchange. This offers additional protection from malicious decryption attempts via "perfect forward secrecy," which means that knowledge of the keys used in one session cannot be used to decrypt future or past sessions.

Many organizations and regulatory bodies are shifting to using and mandating ephemeral key encryption, most commonly Elliptic curve Diffie–Hellman Ephemeral (ECDHE)



To further illustrate the difference, let us consider static keys to be like physical keys—if one is stolen or copied, the person with the key can access all communications locked by that key. In contrast, ephemeral key is like a number generated by a mobile app for a specific exchange. If the number is stolen, it can only be used to unlock that one exchange. All other exchanges are still protected. This perfect forward secrecy is what makes ephemeral key compelling.

Tech industry leaders, including Google, Facebook, Mozilla, and more, are announcing their shift to using ephemeral key for encryption to provide greater security for users. The upcoming TLS 1.3, the latest TLS protocol standard expected to be published in 2017 by the Internet Engineering Task Force (IETF), will increasingly favor ephemeral key exchange.

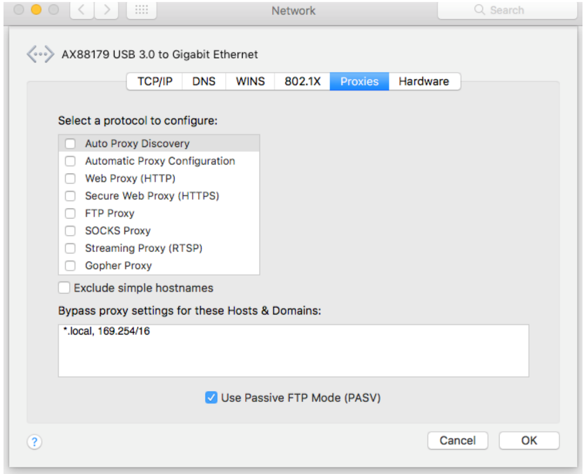
ACTIVE SSL: PREVENTING EPHEMERAL KEY FROM BECOMING A BLIND SPOT

In order to decrypt traffic that has used ephemeral key cryptography for security, troubleshooting, or any other purpose, one must possess the keys used in encrypting the traffic. The only efficient way to gain visibility into traffic encrypted with ephemeral keys, or indeed, any encrypted traffic where one does not possess the relevant encryption keys in advance, is by actively participating in the encrypted connection. This type of connection can be referred to as "Active SSL," because the agent decrypting the traffic is not sitting passively off to the side but is, instead, terminating and generating SSL sessions as an active part of the exchange.

Using Active SSL, also known as an intermediary to both decrypt and re-encrypt traffic, is often referred to as using an "SSL Proxy."

Active SSL or an SSL proxy does the following:

- First, it terminates the SSL connection from the user to a given website, which decrypts traffic to cleartext.
- Then, it observes the decrypted traffic. In most cases, traffic is passed to security and monitoring tools for inspection.
- Once traffic has been inspected, it initiates a new SSL session to the external server, meaning it re-encrypts traffic to send it back onto the original path.



AX88179 USB 3.0 to Gigabit Ethernet

Select a protocol to configure:

□ Auto Proxy Discovery
□ Automatic Proxy Configuration
□ Web Proxy (HTTP)
□ Secure Web Proxy (HTTPS)
□ FTP Proxy
□ SOCKS Proxy
□ Streaming Proxy (RTSP)
□ Gopher Proxy

□ Exclude simple hostnames

Bypass proxy settings for these Hosts & Domains:

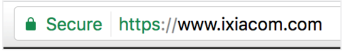
*.local, 169.254/16

☑ Use Passive FTP Mode (PASV)

An Active SSL proxy should not require additional setup by the user or network admin.

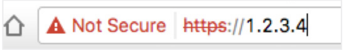
Ideally this is done with low latency and is "transparent to the user"—meaning it does not affect the user experience. The user should not have to perform any additional steps or configure any setup. It should also be transparent to the network infrastructure, again, not requiring reconfiguration of any devices on the network that rely on SSL connections.

When a user opens a browser and opens an encrypted session (HTTPS is HTTP and SSL), the user typically sees a visual indicator, such as the green lock in their browser, which indicates that the connection is encrypted and that the key used at the other end of the connection is trusted.



Secure | https://www.ixiacom.com

If a user connects to a site that has an untrusted encryption key, the user will see a warning, such as the one below:



Not Secure | ~~https~~://1.2.3.4

To make the Active SSL process transparent to the user, the SSL proxy must have an encryption key installed on it that is trusted by the user. In most environments, this is accomplished by inserting the organization's certificate into the user's certificate store when an asset (such as a laptop) is issued. The user may also do a one-time accept of the SSL proxy's certificate. When the user opens a browser and initiates a connection to a secure website, the SSL proxy simply passes packets back and forth until the start of the encryption key exchange is detected. When that occurs, the SSL proxy becomes an active part of the session. It opens a secure session to the external website and, then, inserts its own key into the exchange back to the client. This process is known as "certificate resigning," because it uses the SSL proxy's encryption key, rather than the key of the external site. Because the user's browser trusts the key installed on the SSL proxy, no warnings are given in the browser.

Once the SSL proxy has established SSL connections with both the user's browser and the external server, the connection proceeds as normal from the user's perspective. However, the SSL proxy has access to the cleartext data being shuttled between the two encrypted connections and can make those available for inspection.

SSL DECRYPTION: A TAX ON TOOLS

For proper inspection of traffic, security and monitoring tools need decrypted traffic. Some, but not all, inline security devices can perform the SSL proxy function. However, many organizations use security deployments that conform to the "defense in depth" principle, meaning there are multiple layers of security appliances. It is very inefficient to have multiple devices perform the decryption /re-encryption function, and it adds significant latency. Burdening security devices with the heavy load of encryption can also degrade their performance significantly, by up to 81% in some cases . This also limits security policy capabilities, as the internal SSL proxy cannot make decisions based on criteria, such as the encryption strength of the external server, because it does not have direct visibility. Similarly, an external SSL proxy does not have visibility into internal browser encryption.

When selecting an SSL proxy, it is also important to make sure that it serves the needs of all the connected security, monitoring, and analysis tools while also performing the active SSL function. For example, some tools may require NetFlow data or may be more efficient when inspecting only a single application. Compliance mandates may require any Personally Identifiable Information (PII) present in network traffic be masked prior to archiving. Precision timestamps may be needed for detailed trouble shooting. Many other preprocessing functions may be needed to ensure optimal performance of monitoring and security tools, and it is critical to select an SSL proxy that can perform all of these functions simultaneously.

AN EFFICIENT WAY TO DECRYPT AND RE-ENCRYPT TRAFFIC FOR INSPECTION—IXIA'S ACTIVE SSL ENHANCEMENT TO VISION ONE™

Network packet brokers (NPBs), such as Ixia's Vision ONE, are commonly used as a central visibility hub in security deployments. NPBs are able to flexibly route traffic between multiple sets of security devices and make network traffic available to both inline security devices (such as firewalls and Intrusion Prevention Systems (IPSs)) and out-of-band systems, such as data capture appliances. Vision ONE adds capabilities such as flexible load balancing, service chaining, data masking, and rich NetFlow generation. Because it already has powerful capabilities for connecting and coordinating multiple security devices, a NPB such as Vision ONE is an ideal place to provide "decrypt once, inspect many times" service for all security devices.

Ixia's active SSL capability, available with the turnkey Vision ONE, uses a dedicated, high-performance cryptographic processor. It does not use any resources used by any other function of the Vision ONE platform, such as deduplication, timestamping, rich NetFlow generation, or data masking. The dedicated processor has ample capacity to handle the SSL traffic of enterprise Internet gateways. When combined with all of the advanced functionality already in place on the Vision ONE platform, Ixia's active SSL feature provides an ideal visibility and security hub for all traffic on the network, both cleartext and encrypted.

To learn more, please visit www.ixiacom.com/ActiveSSL.

IXIA WORLDWIDE

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 1.818.871.1805

www.ixiacom.com

IXIA EUROPE

Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127

|