SOLUTION BRIEF

How to Get Ready for TLS 1.3: Ixia's 10-Point Checklist

1. IS YOUR COMPANY CONCERNED ABOUT ENCRYPTED MALWARE BEING DOWNLOADED INTO YOUR NETWORK?

If your IT and security experts are not worried about encrypted security exploits, they should be. Cisco has stated that encrypted traffic has been increasing by more than 90 percent year-over-year, while Gartner states, "through 2019, more than 80% of enterprises' web traffic will be encrypted."[1] Encrypting data makes it much easier for cybercriminals to sneak malware onto your network, and more difficult for firewalls and traditional defenses to detect exploits. Attackers know that many organizations do not inspect encrypted traffic before sending it into their networks, essentially creating a dangerous blind spot.

2. DO YOU CURRENTLY HAVE A WAY TO MONITOR ENCRYPTED COMMUNICATIONS TO YOUR WEB SERVERS?

Many companies do, but implementations and strategies vary widely. For many organizations, adopting the Internet Engineering Task Force's (IETF) newly approved Transport Layer Security (TLS) 1.3 standards for securing encrypted data will mean transitioning from passive monitoring of connections to web servers using Secure Sockets Layer (SSL) technology to employing active decryption, a complex migration with far-reaching implications for the security infrastructure.

ixia
A Keysight Business

1 Gartner, Magic Quadrant for Enterprise Network Firewalls, July 2017

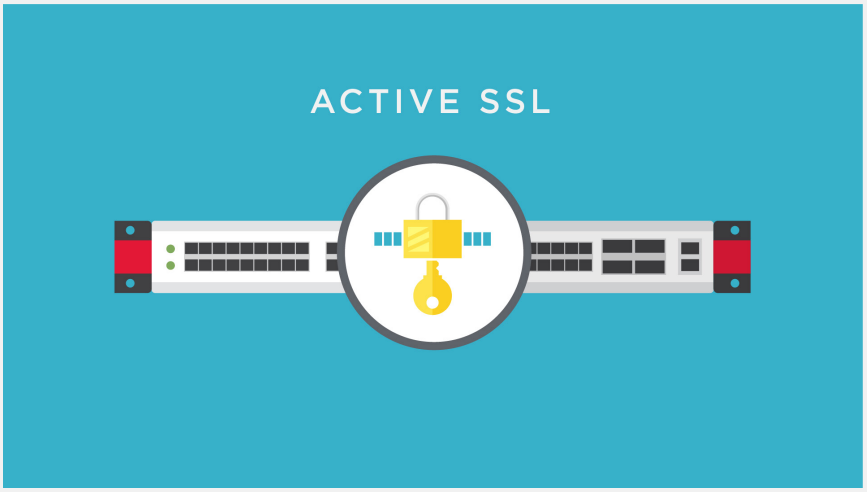
3. DO YOUR FIREWALLS, IPS SOLUTIONS, AND OTHER SECURITY DEVICES PERFORM BOTH PASSIVE AND ACTIVE SSL DECRYPTION?

Previous versions of the SSL and TLS standards for encryption used static keys, which meant each connection between a client and a specific web server used the same key to decrypt data. The upside is that monitoring traffic is easier because you could use your web server's key to encrypt and decrypt network traffic. The downside is that hackers can obtain the key and watch sessions and decrypt traffic for as long as their presence goes undetected and the key remains unchanged.

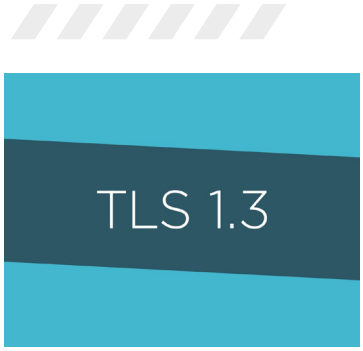
The newly approved TLS 1.3 standard enhances security by using ephemeral or temporary session keys that assign unique decryption keys to each individual server session. This makes it infinitely more difficult for hackers to steal keys in the first place, and ensures that a single stolen key is usable only for a single server session and will not expose future or past connections.

Watch Active SSL Video Here:

https://www.youtube.com/watch?v=QrjxZlNXE1s



4. HOW MIGHT YOUR NETWORK SECURITY BENEFIT FROM ADOPTING THE TLS 1.3 STANDARD FOR SSL DECRYPTION?



TLS 1.3 brings significant benefits versus the current TLS 1.2 standard: Better security and higher performance. The security gain comes from the use of ephemeral keys that make it harder for hackers to snoop and bide their time listening in on encrypted sessions. The performance gain ensues from the fact that, once an initial connection between a client and server has been established, further communications related to that session will execute more quickly.

While the shift to ephemeral keys marks a quantum improvement in terms of security, TLS 1.3 requires decryption solutions to play an active role in processing, which requires some rearchitecting of the overall security infrastructure, particularly for certain industry sectors.

For example, many financial service and healthcare providers required to protect servers and privileged information from theft often monitor and decrypt connections without becoming an active part of the process. They may also stream traffic to a disk so they can go back and decrypt sessions later to take a closer look at activity for a specific account or time frame.

In contrast, social media providers and other companies operating their own web servers may be more focused on upholding user privacy policies than preventing data from being stolen. These companies will no longer be able to secure incoming connections from the Internet using passive SSL inspection and will likely move more quickly to adopt TLS 1.3 and active decryption.

Either way, revamping procedures to adopt active decryption will require significant rearchitecting of security operations.

5. DOES YOUR COMPANY HAVE A PLAN AND BUDGET FOR ADOPTING TLS 1.3?

In terms of timing, Internet browser updates are already underway and will likely be pushed to users by the end of 2018. Web server providers are expected to make software upgrades available in the same time frame. These server upgrades may be free and straightforward for equipment covered by maintenance contracts, but will include disabling older versions of encryption which may take some careful planning.

The more challenging aspect of adopting TLS 1.3 will be rearchitecting the network and security infrastructure to employ active SSL inspection capabilities and monitor connections to web server farms. Companies hosting their own web servers will need to place devices capable of active SSL inspection between users and web server farms, which will mean purchasing new gear and devising a new approach to security.

This evolution could take up to a year depending on the company's business and IT cycles and must be approached methodically to avoid exposing the network to risk. Outsourcing the project to a trusted third party may be a quicker, more cost-effective option.

6. IF YOUR EXISTING SECURITY TOOLS ALREADY SUPPRT ACTIVE SSL, DO YOU KNOW HOW TURNING ON THIS FEATURE WILL IMPACT PERFORMANCE?

Some next generation firewalls and other monitoring devices support active SSL decryption, but decryption is a process-intensive task such that the impact of enabling the feature can reduce overall performance, introduce significant latency, increase the risk of congestion, and require additional capacity in your security infrastructure.

7. DO YOU USE PURPOSE-BUILT TECHNOLOGY TO PERFORM SSL DECRYPTION?

Offloading SSL decryption to standalone solutions or an intelligent visibility infrastructure can exponentially improve efficiency by minimizing the impact on firewalls, IPSs, and other security tools, as well as the number of times traffic must be decrypted and re-encrypted during inspection. Integrating SSL decryption within a visibility infrastructure featuring intelligent network packet brokers (NPBs) alleviates the burden on firewalls without requiring IT to purchase and manage additional point solutions and user interfaces.

8. DO YOU HAVE A WAY TO MEASURE HOW WELL NEW OR UPGRADED SOLUTIONS DETECT ENCRYPTED THREATS?

IT organizations must validate their security devices' ability to support encryption and detect malware and other threats encrypted within application traffic. Specialized security test solutions such as Ixia's BreakingPoint Virtual Edition can be used to generate and transmit encrypted malware and other attacks to help IT evaluate prospective solutions, refine configurations, and measure performance.

As organizations implement TLS 1.3 support across their networks, BreakingPoint offers a cloud-based solution that streamlines multisite testing with a subscription-based pricing model accommodating both project and ongoing IT operations budgets.

9. HOW MANY OF YOUR SECURITY EXPERTS WILL NEED TO SPEND TIME IMPLEMENTING TLS 1.3?

Any fundamental change to the security infrastructure requires careful strategic and logistical planning. Along with upgrading web server software, adopting TLS 1.3 may mean replacing devices that do not support the new standard, and rethinking the way traffic is routed and processed.

With security professionals and expertise already in short supply, solution providers can help IT and security departments develop plans to select new vendors, optimize configurations, and implement TLS 1.3 support while making optimal use of resources and maintenance windows.

10. DO YOU USE NETWORK PACKET BROKERS TO OFFLOAD PROCESSING FROM YOUR SECURITY INFRASTRUCTURE?

Offloading SSL decryption from security devices to an intelligent NPB offers a more efficient and flexible solution than using dedicated standalone inspection appliances. Upon receiving traffic from the network, the NPB can decrypt and forward it for processing by a service chain of best-of-security devices (firewalls, IPS/IDS solutions, data leak protection (DLP) systems, etc.). When processing is complete, the security infrastructure then forwards traffic back to the NPB for re-encryption before sending to internal users, web servers, or the Internet.

Preventing multiple devices in the security chain from having to decrypt and re-encrypt traffic saves time, reduces delay, and conserves processing cycles for specialized processing by each security tool. NPBs also load balance traffic across multiple tools (for example, multiple IPSs) to keep all devices working at peak functionality. When combined with bypass switching—another core element of an intelligent network visibility architecture—the NPB helps to automatically reroute traffic around devices that have failed or been taken out of service for maintenance to keep traffic flowing safely during planned or unplanned outages.

Compared with using standalone decryption appliances, integrated visibility solutions support flexible service chains, the ability to combine inline and out-of-band security tools, failure detection, Netflow generation, and other capabilities—all managed through a single user interface (UI).

Learn more at: www.ixiacom.com

For more information on Ixia products, applications, or services, please contact your local Ixia or Keysight Technologies office. The complete list is available at: www.ixiacom.com/contact/info

915-8284-01-6081 Rev A