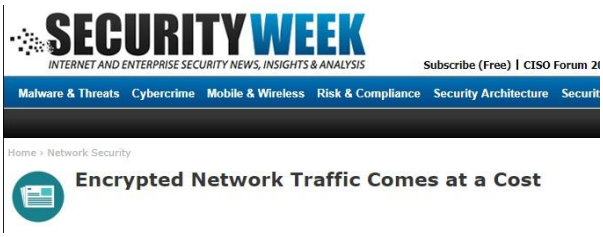
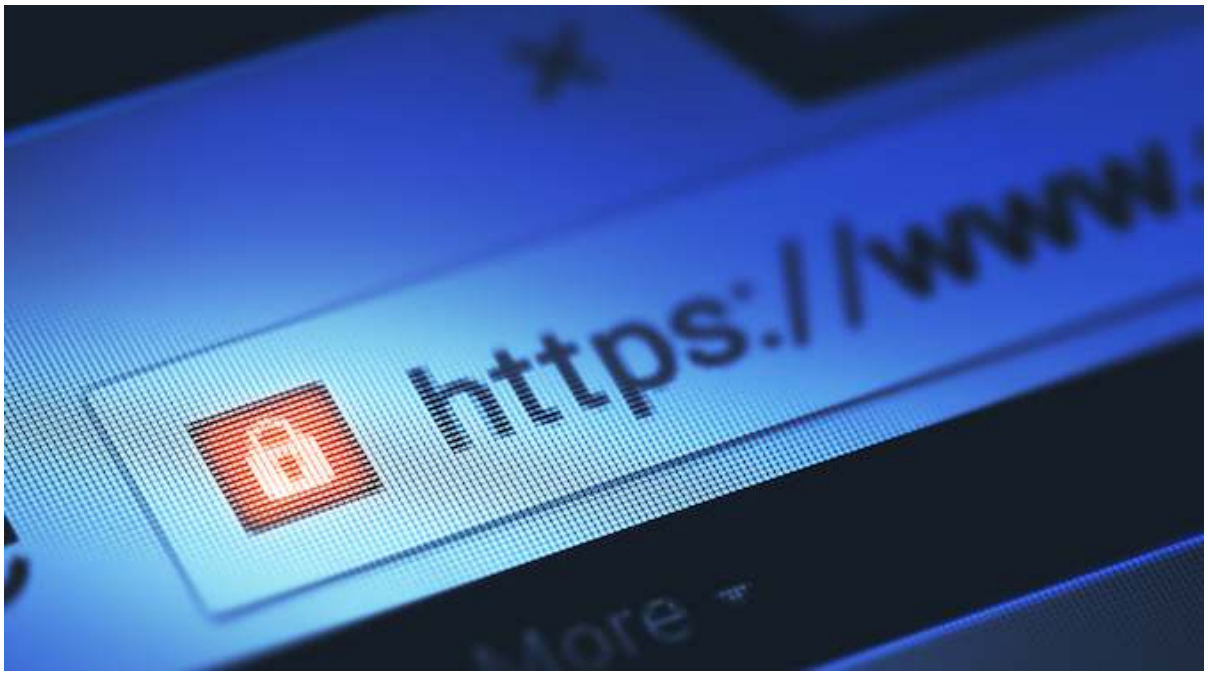


Encrypted Network Traffic Comes at a Cost

Tags: Network Security NEWS & INDUSTRY

6-8 minutes



SSL/TLS Encrypted Network Traffic Brings Privacy for Users and Headaches for Security Teams

The use of encryption over the Internet is growing. Fueled by Edward Snowden's revelations on the extent of NSA and GCHQ content monitoring, encryption is now increasingly provided by the big tech companies as part of their standard product offerings. It's effectiveness can be seen in the continuing demands by different governments for these same tech companies to provide government backdoors for that encryption. Encryption works: it

safeguards privacy.

Against this background, the use of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to encrypt network traffic is likely to grow dramatically. Google is encouraging this. It already uses HTTPS as a positive weight for web sites in its search algorithm, while current rumors suggest it will soon start to place a warning red X in the URL bar of sites that do not use it. Taken together, these are strong incentives for businesses that don't currently use SSL/TLS to start doing so. Some predictions believe that almost 70% of network traffic will be encrypted by the end of this year.

But SSL and TLS traffic encryption brings its own problems for businesses. Encryption is already used by criminals to hide malicious traffic on the basis that defenders cannot find what they cannot see. Enterprises are already forced to decrypt encrypted traffic at the gateway in order to inspect and determine whether it is safe or harmful.

A10 Networks' Rene Paap, who expects 67% of all network traffic to be encrypted by the end of this year, thinks this will place an intolerable demand on existing firewalls.

Herein lies the issue: If you encrypt less, attackers can spy on your traffic and Google could put you in the penalty box. If you encrypt more, you'll need to decrypt everything so that your security systems will still work.

This is already a practical problem. Martin Zinaich, information security officer for the City of Tampa and a founding member of the Wisegate community of security officers, explains that it all started with Firesheep, a Firefox extension that allows users to steal session cookies. After Firesheep, he told *SecurityWeek*, most large websites went to full-on SSL encryption. Sites like Google, Twitter, and Facebook all went to SSL for the complete user session. This also meant that security professionals lost deep packet inspection, as the traffic payloads were encrypted. Whether they realized it or not, the amount of traffic they could inspect almost immediately went down drastically."

The solution is to decrypt the traffic before it gets into the local network – but it is computationally very heavy. "The client connects to a certificate they trust (SSL), the traffic is decrypted, inspected and another connection is made to the target where the traffic is encrypted and sent (again over SSL). This takes a lot of overhead," explained Zinaich, adding, "I know two colleagues who gave up after having numerous performance problems."

If firewalls are struggling to cope now, there will be serious problems as SSL/TLS traffic increases. The right solution, suggests Shehzad Merchant, CTO of Gigamon, "is to move from a scale up model to a scale out model." Rather than allow a single device like a firewall to become the central bottleneck for all functions (firewall, UTM, sandbox, decryption, etc.) those functions should be distributed out. "That way," continues Merchant, "only the right traffic hits the specific functions allowing the solutions to scale much better, improve latency and increase resiliency. Functions like decryption are no different. By moving decryption into a platform that serves all the different security functions in a scale out manner

i.e. decrypt once then distribute traffic across the various security functions that need the decrypted traffic, performance issues can be addressed."

Zinaich points to an additional problem. "If security professionals are deploying SSL inspection, they better be working with the company's legal staff," he said, "because now they can see all login information sent from any user to any website. Who is going to have access to this information? Where is it going to be stored? How will it be secured? SSL inspection is another bolt-on reactive security measure for a broken base protocol implementation, but it's the only way to inspect encrypted traffic."

Both of these issues were endorsed by A10 Networks' Rene Paap. The crypto functions need to be handed off from the firewall to a separate specialist device that can integrate seamlessly with it. But that device also needs to understand financial and healthcare regulations so that at least the sensitive PII can bypass the encryption and stay hidden.

Some experts say there is no real choice. "Yes, encrypting network traffic does present some challenges," confirmed F-Secure's Sean Sullivan. "So, perhaps there are some advantages for attackers – but the drive for encryption is good for our customers in the bigger picture. If we (as AV/endpoint vendors) have to work harder, it wouldn't be the first time. There has always been an evolving threat landscape to deal with."

Ivan Ristic, a security researcher and author of SSL Labs, agrees that increased security is worth the increased cost. "If there's no encryption there's no security," he told *SecurityWeek*. "It's simple as that. You can forego encryption if you don't care about security and

your systems will be super-fast. But, if you do care, there's no choice but to encrypt."

**Correction - Incorrectly attributed statement in paragraph five to A10's Paap.*

Related Reading: SSL Encryption: Keep Your Head in the Game

Related Reading: To Improve Security Effectiveness, Look Inside

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend: