Return to the VPLS Blog

Blog Post

Eliminating Firewall Blind Spots with SSL Decryption

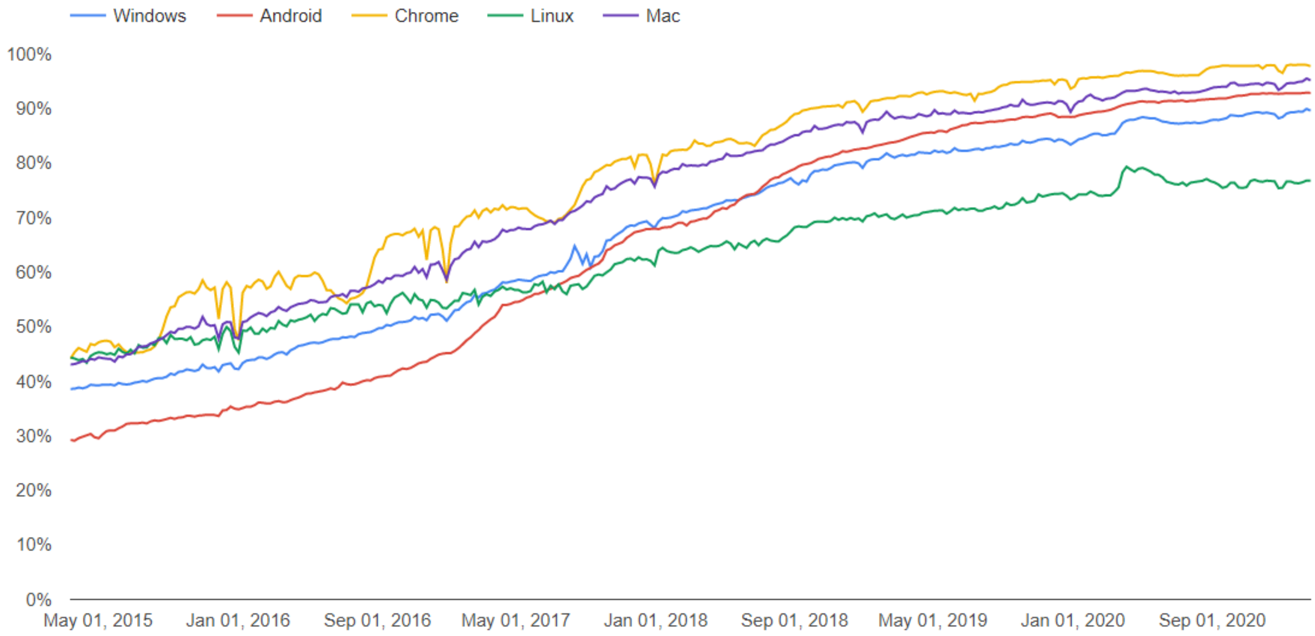
Published
Feb 18, 2021

Written by
John Headley

Filed under
Cybersecurity, Firewall, Fortinet

For years, it was common to visit websites that were not available over HTTPS, and even as recent as 2019, major websites like ESPN were still only available over regular, insecure HTTP. However, thanks to initiatives from web browsers, like Google Chrome in 2018 who began warning users that any website visited over HTTP is “not secure”, encountering a website that is only available via HTTP is a rare occurrence these days. In fact, according to Google, Chrome users are now spending more than 90 percent of their time using encrypted websites and applications.

This astounding statistic makes it clear that encrypted traffic has become the new normal. As a user, this statistic represents an amazing shift forward in regards to privacy and security, but as an IT and cybersecurity professional, this brings new challenges: is your firewall effective against traffic that is, by design, supposed to keep prying eyes out?



Percentage of pages loaded over HTTPS in Chrome by platform

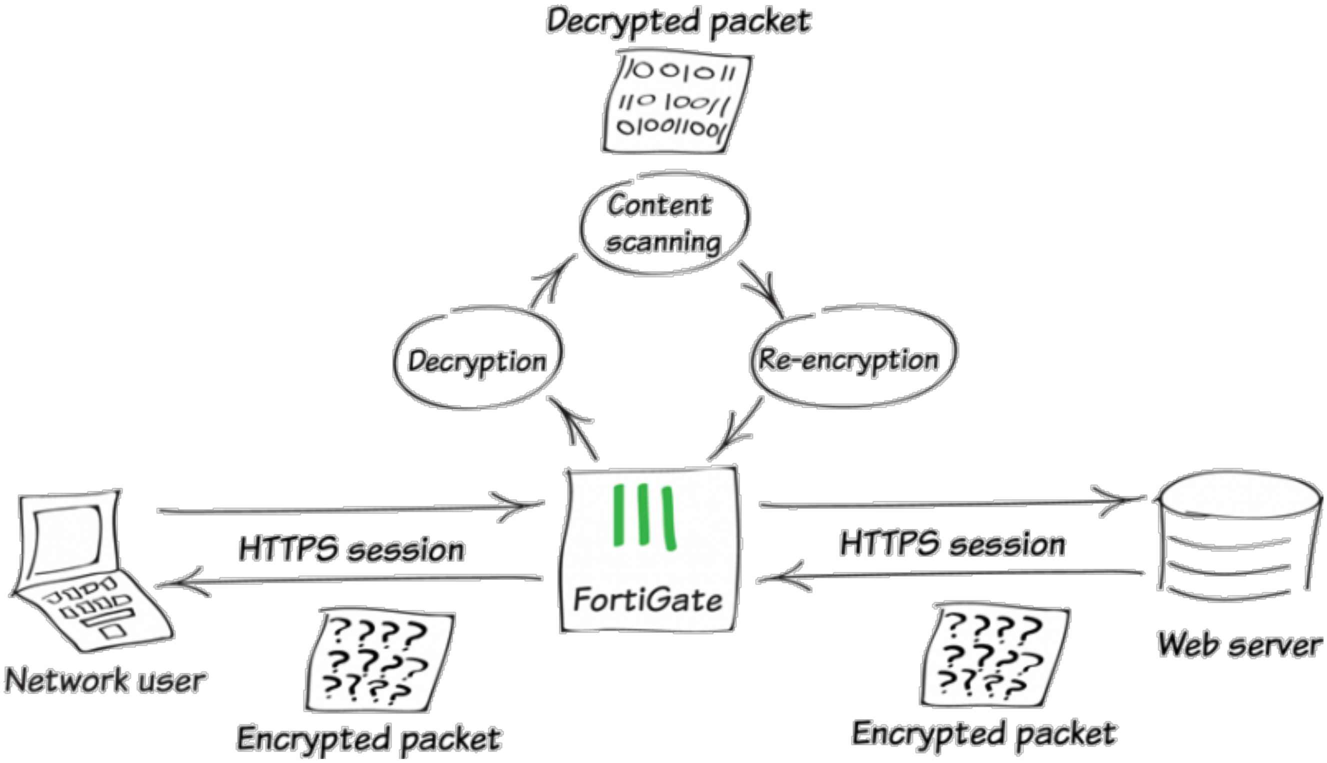
How can SSL create a blind spot?

Secure Sockets Layer (SSL), later replaced by Transport Layer Security (TLS), is the standard protocol to transmit secure data over the internet. It is what makes visiting a website over HTTPS secure versus plain HTTP. SSL encrypts traffic, placing it inside of a “tunnel” so the confidentiality and integrity of your banking transaction, for example, remain unaffected.

Unfortunately, this technology was designed for good, but can also be used for evil, as cybercriminals commonly hide threats inside of encrypted traffic in order to go around security controls. Even businesses with the most extensive security measures in place can be targeted if they are not closely monitoring encrypted traffic.

Solution: SSL Decryption

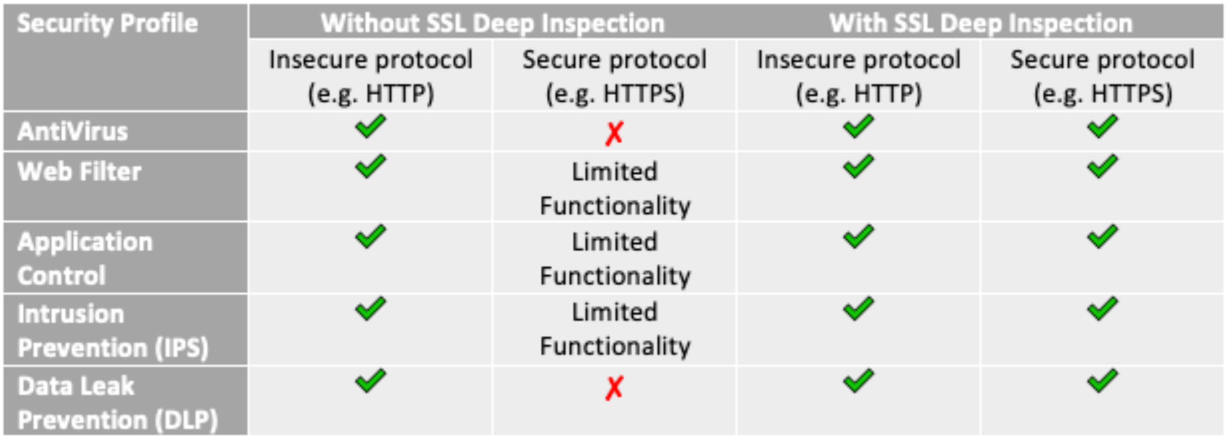
On a next-gen firewall like a Fortinet FortiGate, the key to monitoring and protecting against threats that may be contained inside encrypted traffic is SSL decryption, also commonly called SSL deep packet inspection. With SSL decryption enabled, the firewall is configured to intercept encrypted traffic before it reaches its destination. Once intercepted, the firewall will decrypt, inspect, and re-encrypt the traffic before forwarding it to the original destination. SSL decryption gives the firewall new capabilities to identify and analyze encrypted traffic and applications to prevent these previously undetectable threats, attacks, and data leakage.



SSL decryption is a very powerful capability, and in some cases regulations may prohibit you from decrypting user data. In these cases, the firewall can be configured to decrypt HTTPS only on certain questionable websites and applications, while other web traffic from familiar and recognizable organizations smoothly bypasses SSL decryption.

Firewall Limitations Without SSL Decryption

Without SSL decryption, the security profiles on your next-gen firewall are limited in their ability to protect you against these hidden threats. The table below gives an example of how a FortiGate next-gen firewall's features are limited when SSL deep inspection is not enabled:



Security Profile	Without SSL Deep Inspection		With SSL Deep Inspection	
	Insecure protocol (e.g. HTTP)	Secure protocol (e.g. HTTPS)	Insecure protocol (e.g. HTTP)	Secure protocol (e.g. HTTPS)
AntiVirus	✓	✗	✓	✓
Web Filter	✓	Limited Functionality	✓	✓
Application Control	✓	Limited Functionality	✓	✓
Intrusion Prevention (IPS)	✓	Limited Functionality	✓	✓
Data Leak Prevention (DLP)	✓	✗	✓	✓

And these firewall limitations don't just apply to HTTP and HTTPS traffic. Other secure protocols can be inspected with SSL deep inspection as well, such as

SMTPS, POP3S, IMAPS, and FTPS.

If your organization is unsure if your firewall is performing SSL decryption, or if you want expert guidance on enabling SSL decryption, please reach out to us. We are happy to offer a free consultation on how our team of certified security experts can help give you the visibility needed in today's world of almost completed encrypted traffic.

Need SSL Decryption?

Connect with a VPLS expert to get answers about any of our cybersecurity services.

Reach Out Now

Read More from this Author

John Headley

John Headley, CISSP and Fortinet NSE8 #003155, is a Senior Security Engineer at VPLS where he splits his time between both pre-sales and post-sales engagements. His expertise is in security architecture and engineering, security assessment and compliance, and security operations. During his time at VPLS, he has led many security-related professional services projects, including a 35-location international firewall deployment for a publicly-traded social media company.

More from this Author

‹ PREVIOUS
Who is the Insider Threat?

NEXT ›
An Engineer’s Perspective on Managed Firewalls

If you enjoyed this article, you'll probably like:

BLOG POST
5 Reasons SOC-as-a-Service
Will Give You Peace of Mind
If you're not sure if outsourcing your SOC is worth it, here are some SOC-as-a-Service features that provide peace of mind
READ NOW

5 Reasons SOC-as-a-Service Features Help You

March 29, 2022

Read More »

BLOG POST
What is SOC-as-a-Service?
SOC-as-a-Service (SOCaaS) functions as an extension of a company's IT department and helps take the guesswork out of cybersecurity.
READ NOW

What Is SOC-as-a-Service?

March 28, 2022

Read More »

BLOG POST
VDI vs. VPN
What's Best for Remote Employees?
Many companies struggle with deciding which of these two common remote work is better for their workforce.
READ NOW

VDI vs. VPN: What’s Best for Remote Employees?

February 14, 2022

Read More »

HOW TO REACH US

Corporate Headquarters
600 West 7th Street, Suite 510
Los Angeles, CA 90017

24/7/365 Customer Service
+1 (888) 365-2656
support@vpls.com

Sales Inquiries
+1 (888) 365-2656
sales@vpls.com

WHAT WE DO

Cloud
Hosting
Colocation
Network Services
Managed Services
Professional Services
VAR

WHO WE SERVE

Financial Services
Healthcare and Life Sciences
Media & Entertainment
Telecom
Startup
Enterprise
Public Sector