Firewall Scalability: Using SSL vs Clear Text

Roughly 80% of web traffic is encrypted. However, performance can drop significantly when decryption is enabled on a firewall.

Knowing this, vendors disable decryption by default. Therefore, we felt it was important to provide in-depth metrics and help you plan for scaling your network when content is encrypted using SSL vs. Clear Text.

KEY FINDINGS

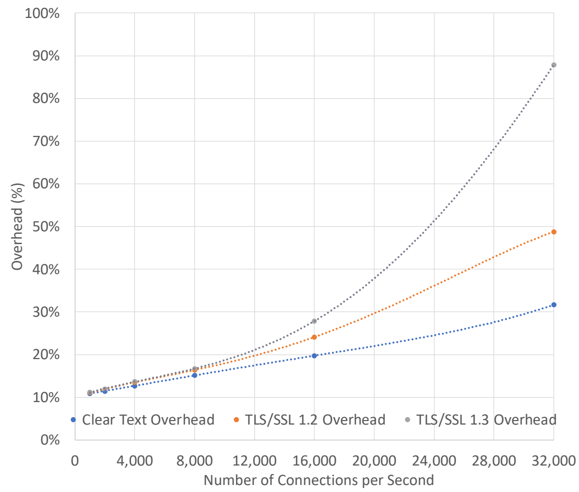
- Roughly 80% of web traffic is encrypted, yet firewalls have encryption turned off by default.
- If an attack is encrypted but firewall encryption/decryption for TLS/SSL is not enabled, the firewall will not see the attack, which will pass through the firewall's protection unimpeded.
- Customers are not enabling encryption/decryption for TLS/SSL because:
    - they are unaware that they need to turn it on
    - they are concerned about the (unknown) performance impact.
- There is a general lack of public knowledge when it comes to scaling encrypted traffic.
    - It is standard practice to rate firewall performance using unencrypted traffic.
    - It is standard practice for performance numbers to reflect the *total data transferred* not the *usable content transferred* (e.g., web page content).

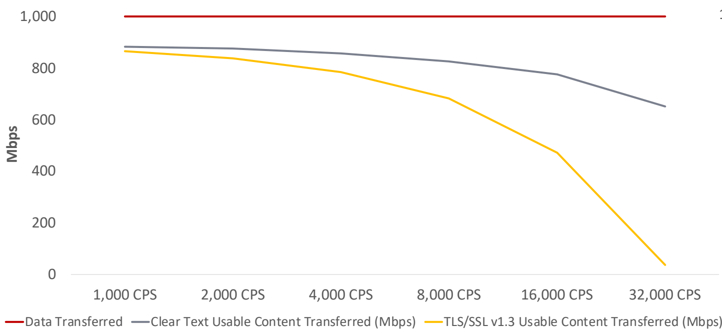
RECOMMENDATIONS

- Identify desired encryption cipher suites based on the sensitivity of content and regulations.
- When capacity planning, use TLS/SSL performance measurements for both total data and usable content transferred (e.g., how many people can visit your web page simultaneously if it is encrypted using TLS 1.3 vs. unencrypted / cleartext).
- Determine the range of content (payload) sizes, both current and planned, encrypted and unencrypted; calculate capacity requirements accordingly.
- Calculate content to overhead ratio using your content and desired cipher suites. If your overhead is excessive:
    - Using a dedicated SSL offloading device might be an option.
    - Look to leverage content delivery networks.
    - Speak to developers about optimizing for network considerations.
- Turn on TLS/SSL encryption/decryption.

EXECUTIVE OVERVIEW

When a client and server connection is established to deliver a payload (content), additional data is transferred to ensure delivery: prioritize certain content, do error checking, encrypt, negotiate communications (handshake), adjust for packet loss, etc. This overhead means that in 1 Gbps of transmitted traffic, only a portion of that traffic is the content you are trying to deliver.





In the figure on the left, we see how content transferred declines when the number of connections increases. Since the overhead is constant for each connection, increasing the connections per second means less bandwidth for content.

CONNECTIONS PER SECOND

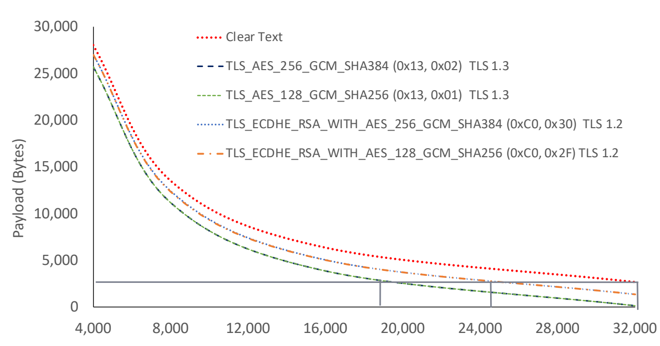
Most people think about download speed in megabits per second (Mbps). For firewalls, however, connections per second are much more critical since firewalls track connections; firewalls do not track webpages, images, audio, movies, etc.

The table below details the overhead for clear text and TLS/SSL 1.3. The amount of overhead used for TLS/SSL is mainly due to the handshake (exchange of encryption keys). As a result of this added overhead, the firewall content delivery (performance) efficiency decreases.

CPS	Clear Text [HTTP]		TLS_AES_128_GCM_SHA256 [(0x13, 0x01) TLS 1.3]	
	Content	Overhead	Content	Overhead
1,000	89%	11%	89%	11%
2,000	89%	11%	88%	12%
4,000	87%	13%	86%	14%
8,000	85%	15%	83%	17%
16,000	80%	20%	72%	28%
32,000	68%	32%	12%	88%

In this paper, we provide steps for how to apply these calculations in your environment. For example, by knowing the payload size, i.e., 2,667 Bytes, we can determine the maximum CPS clear text, TLS/SSL 1.2, and TLS/SSL 1.3:

Clear Text max: ~ 32,000 CPS | ~ 651 Mbps
TLS/SSL 1.2 max: ~ 25,000 CPS | ~ 509 Mbps
TLS/SSL 1.3 max: ~ 19,000 CPS | ~ 387 Mbps



WHY DO CONNECTIONS PER SECOND MATTER?

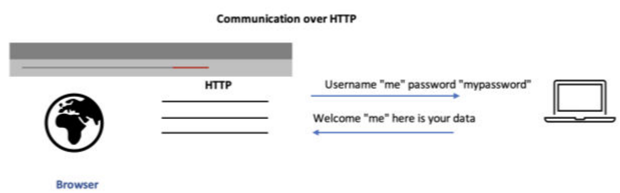
As of 2023 most traffic passing through a firewall is web traffic. Here is how the communication between a user and a web server occurs:

The communication between the browser (client) and website (server) happens through clear text (HTTP) requests and responses. An HTTP request is a communication request sent by the client to the server. The server then processes this request and returns the response to the client, known as an HTTP response.

Unfortunately, anyone monitoring an HTTP session can read the information being transferred. This creates a potential security threat. Encrypting traffic prevents an unauthorized third party from reading the information being transferred.

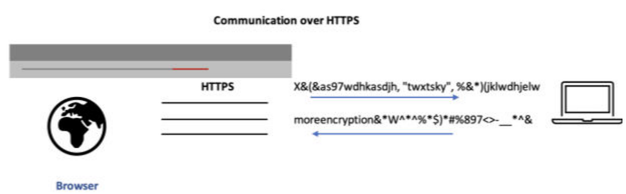
HTTP + TLS/SSL

When HTTP is combined with an encryption protocol such as TLS/SSL, it is known as HTTPS. This is because it encrypts the data retrieved by HTTP protocol and ensures that any third person cannot read the information transferred between the client and servers – with the help of encryption algorithms.



HTTPS

HTTPS provides bidirectional encryption between client and server (encrypts and decrypts the browser requests and server responses). This process is known as a handshake, which ensures that both are the devices they claim to be and protects against man-in-the-middle attacks, eavesdropping, and tampering with the transmission. If a hacker sees the communication, the hacker will only see mixed characters, which are nearly impossible to decrypt or read.



HTTP VS. HTTPS PERFORMANCE

How do clear text and TLS/SSL differ from a performance perspective?

On paper, HTTP is faster than HTTPS due to its simplicity, since in HTTPS, we have an additional step of the SSL handshake. This extra step slightly delays the website's page load speed (latency). However, from a web server and a user perspective, this is highly dependent upon things like the length of the session, the ratio of static vs. dynamic content, caching behavior of the client, content delivery networks, hardware, server software, etc.

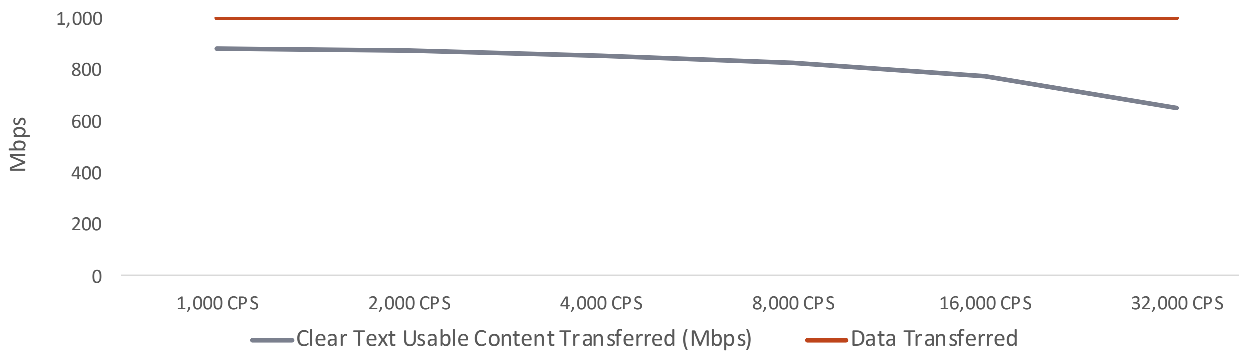
Furthermore, HTTP/2 and other optimizations can render HTTPS pages as fast as those using HTTP. This is not something we address in this paper; however, web developers should consider the impact to firewalls when building their websites, APIs, etc. How they use HTTP/2, content delivery networks, compression, TLS session reuse, keep alive, etc., can have a big impact on performance.

DOING THE MATH

Now that you know your network dynamics (connections per second, min/max/average content size, concurrent connections, etc.), it is time to figure out what you can expect. The table below outlines the number of connections per second, with a fixed content size, at which a firewall can theoretically perform. The test was set to 1 Gbps (Gigabit per Second).

CLEAR TEXT

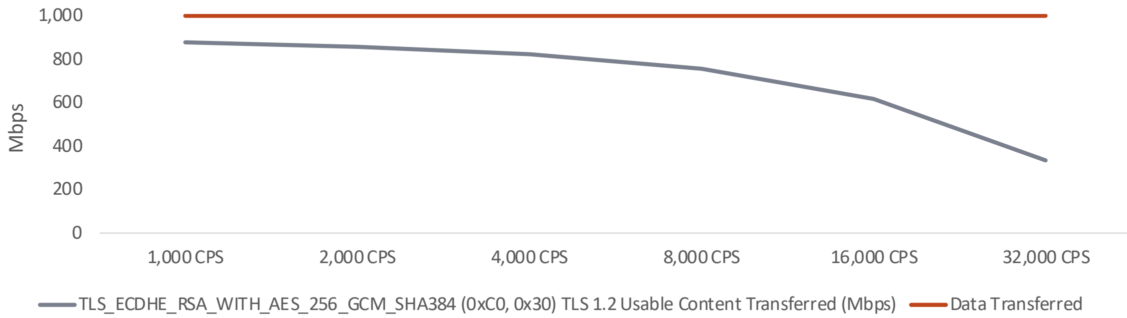
To calculate how fast the firewall can transfer the data, we convert the content from Bytes to Bits, then to Bits per second, and finally to Megabits per second. These are the clear text performance limitations using HTTP.



Clear text										
CPS	Content (HTML)				Total HTTP				Total Transfer	
	Response Size (Bytes)	Bits	Bits per second	Mbps	Response Size (Bytes)	in Bits	Bits per second	Mbps	Content	Overhead
1,000	115,570	924,56	924,560,0	882	129,738	1,037,9	1,037,904,0	990	89%	11%
2,000	57,388	459,10	918,208,0	876	64,824	518,592	1,037,184,0	989	89%	11%
4,000	28,048	224,38	897,536,0	856	32,136	257,088	1,028,352,0	981	87%	13%
8,000	13,512	108,09	864,768,0	825	15,920	127,360	1,018,880,0	972	85%	15%
16,000	6,353	50,824	813,184,0	776	7,916	63,328	1,013,248,0	966	80%	20%
32,000	2,667	21,336	682,752,0	651	3,903	31,224	999,168,00	953	68%	32%

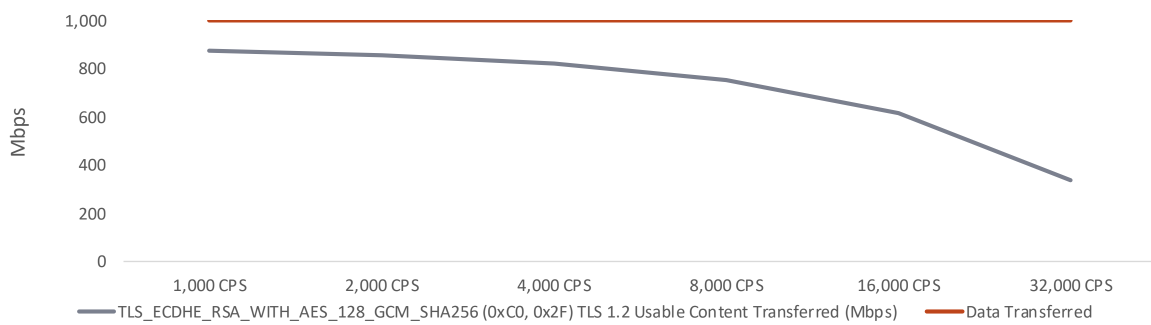
The following charts provide calculations for the most used TLS/SSL 1.2 and TLS/SSL 1.3 cipher suites.

TLS/SSL 1.2 (0xC0, 0x30)



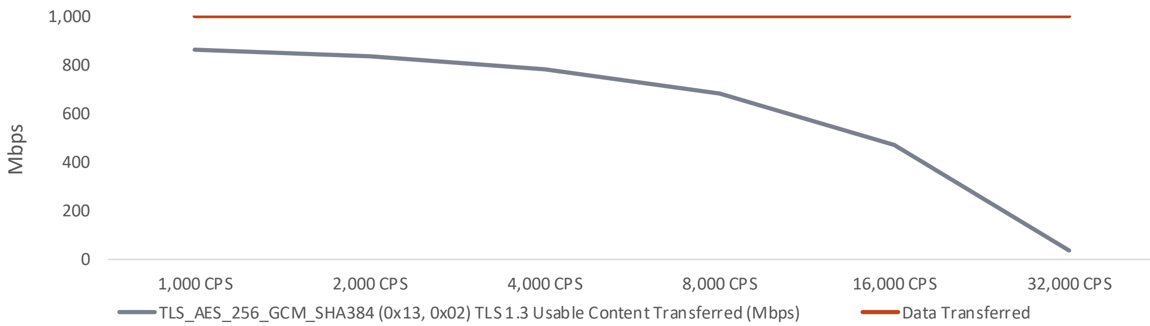
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30) TLS 1.2										
CPS	Content (HTML)				Total HTTPS				Total Transfer	
	Response Size (Bytes)	Bits	Bits per second	Mbps	Response Size (Bytes)	in Bits	Bits per second	Mbps	Content	Overhead
1,000	115,000	920,00	920,000,0	877	129,360	1,034,880	1,034,880,0	987	89%	11%
2,000	56,257	450,05	900,112,0	858	63,945	511,560	1,023,120,0	976	88%	12%
4,000	26,970	215,76	863,040,0	823	31,047	248,376	993,504,00	947	87%	13%
8,000	12,394	99,152	793,216,0	756	14,808	118,464	947,712,00	904	84%	16%
16,000	5,047	40,376	646,016,0	616	6,738	53,904	862,464,00	823	75%	25%
32,000	1,365	10,920	349,440,0	333	2,605	20,840	666,880,00	636	52%	48%

TLS/SSL 1.2 (0xC0, 0x2F)



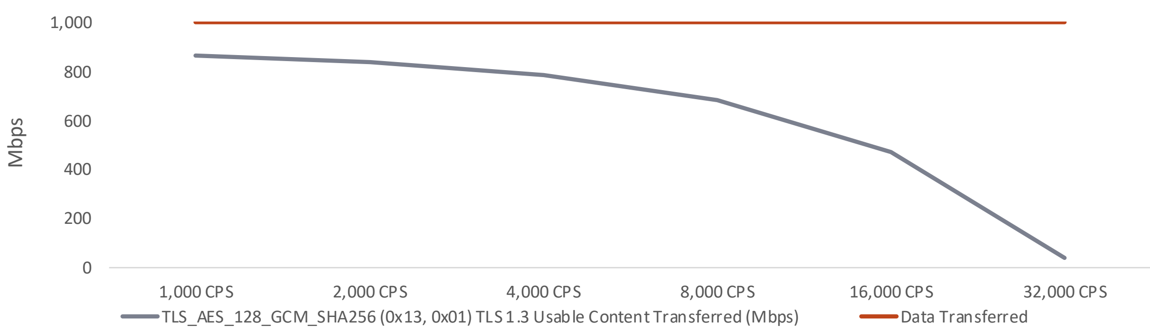
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F) TLS 1.2										
CPS	Content (HTML)				Total HTTPS				Total Transfer	
	Response Size (Bytes)	Bits	Bits per second	Mbps	Response Size (Bytes)	in Bits	Bits per second	Mbps	Content	Overhead
1,000	115,000	920,00	920,000,0	877	129,358	1,034,864	1,034,864,	987	89%	11%
2,000	56,257	450,05	900,112,0	858	63,863	510,904	1,021,808,	974	88%	12%
4,000	26,981	215,84	863,392,0	823	31,204	249,632	998,528,0	952	86%	14%
8,000	12,337	98,696	789,568,0	753	14,756	118,048	944,384,0	901	84%	16%
16,000	5,047	40,376	646,016,0	616	6,651	53,208	851,328,0	812	76%	24%
32,000	1,380	11,040	353,280,0	337	2,694	21,552	689,664,0	658	51%	49%

TLS/SSL 1.3 (0x13, 0x02)



TLS_AES_256_GCM_SHA384 (0x13, 0x02) TLS 1.3										
CPS	Content (HTML)				Total HTTPS				Total Transfer	
	Response Size (Bytes)	Bits	Bits per second	Mbps	Response Size (Bytes)	in Bits	Bits per second	Mbps	Content	Overhead
1,000	113,430	907,44	907,440,0	865	127,666	1,021,328	1,021,328,0	974	89%	11%
2,000	54,917	439,33	878,672,0	838	62,455	499,640	999,280,00	953	88%	12%
4,000	25,700	205,60	822,400,0	784	29,710	237,680	950,720,00	907	87%	13%
8,000	11,170	89,360	714,880,0	682	13,483	107,864	862,912,00	823	83%	17%
16,000	3,870	30,960	495,360,0	472	5,358	42,864	685,824,00	654	72%	28%
32,000	150	1,200	38,400,00	37	1,227	9,816	314,112,00	300	12%	88%

TLS/SSL 1.3 (0x13, 0x01)



TLS_AES_128_GCM_SHA256 (0x13, 0x01) TLS 1.3										
CPS	Content (HTML)				Total HTTPS				Total Transfer	
	Response Size (Bytes)	Bits	Bits per second	Mbps	Response Size (Bytes)	in Bits	Bits per second	Mbps	Content	Overhead
1,000	113,430	907,44	907,440,00	865	127,781	1,022,24	1,022,248,0	975	89%	11%
2,000	54,917	439,33	878,672,00	838	62,381	499,048	998,096,00	952	88%	12%
4,000	25,700	205,60	822,400,00	784	29,781	238,248	952,992,00	909	86%	14%
8,000	11,170	89,360	714,880,00	682	13,413	107,304	858,432,00	819	83%	17%
16,000	3,870	30,960	495,360,00	472	5,365	42,920	686,720,00	655	72%	28%
32,000	150	1,200	38,400,000	37	1,239	9,912	317,184,00	302	12%	88%

CALCULATE CONNECTIONS PER SECOND

As we previously pointed out, when you know your payload size, i.e., 2,667 Bytes, we can determine the maximum CPS clear text, TLS/SSL 1.2, and TLS/SSL 1.3:

- Clear Text max: ~ 32,000 CPS | ~ 651 Mbps
- TLS/SSL 1.2 max: ~ 25,000 CPS | ~ 509 Mbps
- TLS/SSL 1.3 max: ~ 19,000 CPS |~ 387 Mbps

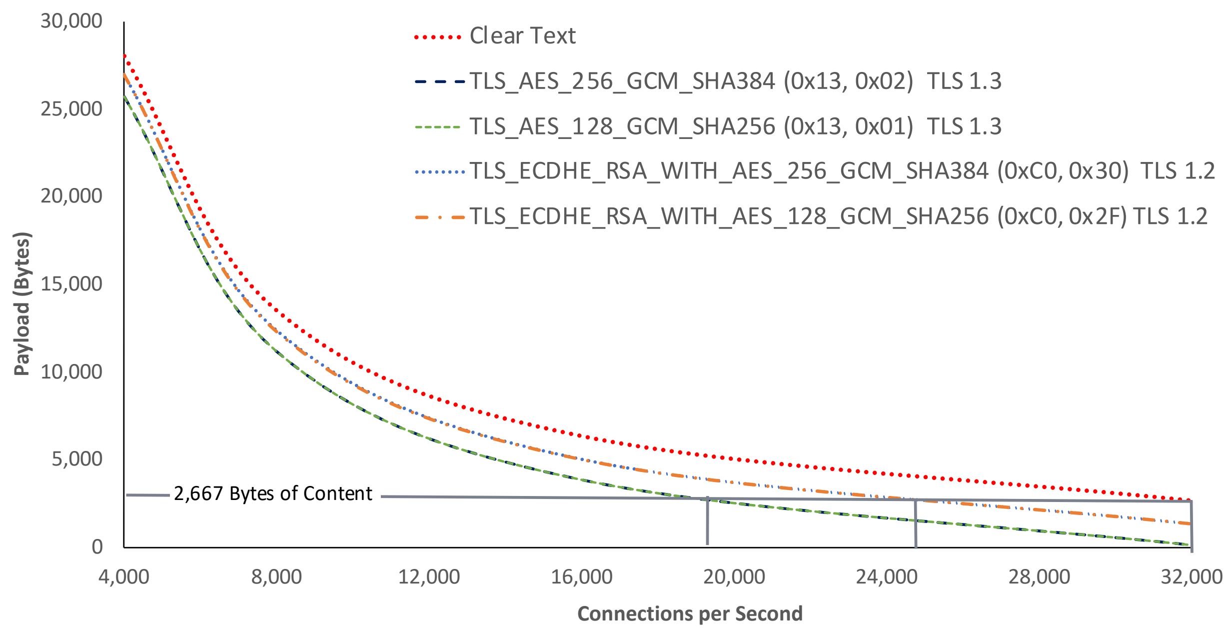
In the below figure, we plotted the usable content from 4,000 to 32,000 connections per second. This estimates how many connections per second and usable content you can expect to achieve.

Starting with a clear text example, the math will be as follows:

> (32,000 Connections per second * 2,667 Bytes of content) *8 = 682,752,000 (total usable content in bits per second) 682,752,000/ (1024*1024) = 651 Mbps (total usable content in Megabits per second)

Using either of the TLS/SSL 1.3 ciphers, the math will be as follows:

> (19,000 Connections per second * 2,667 Bytes of content) *8 = 405,384,000 (total usable content in bits per second) 405,384,000 / (1024*1024) = 387 Mbps (total usable content in Megabits per second)



AUTHORS

Thomas Skybakmoen, Vikram Phatak

CONTACT INFORMATION

CyberRatings.org

2303 Ranch Road 620 South

Suite 160, #501

Austin, TX 78734

info@cyberratings.org

www.cyberratings.org