SSL/TLS PERFORMANCE TEST REPORT

Fortinet FortiGate 500E v5.6.3GA build7858

JULY 17, 2018

Authors – Devon James, Michael Shirley, Tim Otto

This report is Confidential and is expressly limited to NSS Labs' licensed users.

Overview

NSS Labs performed an independent test of the Fortinet FortiGate 500E v5.6.3GA build7858. The product was subjected to thorough testing at the NSS facility in Austin, Texas, based on the SSL/TLS Performance Test Methodology v1.3, which is available at www.nsslabs.com. This test was conducted free of charge and NSS did not receive any compensation in return for Fortinet's inclusion.

This report provides detailed information about this product and its SSL/TLS performance. Additional information about the product's next generation firewall (NGFW) capabilities is available at www.nsslabs.com.

NSS research has found that the use of HTTPS has risen significantly over the past few years; web browser-based applications such as Facebook and Twitter and search engines such as Google are enabling SSL by default as a result of privacy and security concerns. In 2016, NSS research found that HTTPS (SSL/TLS-encrypted) traffic grew 90% year over year and that 50% of enterprise traffic was encrypted. Furthermore, NSS projects that this percentage will rise to 75% in 2019. With this increase in SSL/TLS traffic, enterprises are seeing performance impacts on their NGFWs. This test report covers the 30 most common Cipher Suites from the Alexa Top 1 Million, as of 12/31/2017. Figure 1 presents the overall results of the test.

Product		NSS-Tested SSL/TSL Throughput (Mbps)	SSL/TLS Functionality
Fortinet FortiGate 500E v5.6.3GA build7858		5,773	45/45
Decrypt Top 30 Ciphers	Block Payload	Decrypt Emergent Ciphers	Block Weak Ciphers
30/30	PASS	2/2	PASS
Decryption Bypass Exceptions	Certificate Validation	Session ID Re-Use	Session Ticket Re-Use
PASS	PASS	PASS	PASS

Figure 1 – Overall Test Results

The FortiGate 500E is rated by NSS at 5,773 Mbps with SSL/TLS enabled.

NSS-Tested SSL/TLS Throughput is calculated as a weighted average of the SSL/TLS traffic that NSS expects an NGFW to experience in an enterprise environment. The device supports all SSL/TLS functionality tested. For more details on SSL performance, please see *Appendix: Scorecard*.

Table of Contents

Overview **2**

SSL/TLS **7**

SSL/TLS Functionality 7

Decryption Validation *7*

Cipher Selection *7*

Cipher Support *8*

Top 30 Cipher Suites from the Alexa Top 1 Million, as of 12/31/2017 ..... *8*

TLS ECDHE RSA WITH AES 256 GCM SHA384 ..... *8*

TLS ECDHE RSA WITH AES 128 GCM SHA256 ..... *9*

TLS ECDHE ECDSA WITH AES 128 GCM SHA256 ..... *9*

TLS ECDHE RSA WITH AES 256 CBC SHA384 ..... *9*

TLS DHE RSA WITH AES 256 GCM SHA384 ..... *10*

TLS ECDHE RSA WITH AES 256 CBC SHA *10*

TLS DHE RSA WITH AES 256 CBC SHA *10*

TLS RSA WITH AES 256 CBC SHA *10*

TLS RSA WITH AES 128 CBC SHA *11*

TLS RSA WITH AES 256 CBC SHA256 ..... *11*

TLS RSA WITH AES 256 GCM SHA384 ..... *11*

TLS ECDHE RSA WITH AES 128 CBC SHA256 ..... *11*

TLS RSA WITH AES 128 CBC SHA256 ..... *12*

TLS RSA WITH RC4 128 SHA *12*

TLS RSA WITH AES 128 GCM SHA256 ..... *12*

TLS ECDHE RSA WITH AES 128 CBC SHA *12*

TLS ECDHE ECDSA WITH AES 256 GCM SHA384 ..... *13*

TLS RSA WITH RC4 128 MD5 ..... *13*

TLS ECDHE RSA WITH RC4 128 SHA *13*

TLS DHE RSA WITH AES 128 CBC SHA *13*

TLS DHE RSA WITH AES 128 GCM SHA256 ..... *14*

TLS RSA WITH 3DES EDE CBC SHA *14*

TLS DHE RSA WITH AES 256 CBC SHA256 ..... *14*

TLS DHE RSA WITH CAMELLIA 256 CBC SHA *14*
TLS DHE RSA WITH SEED CBC SHA *15*
TLS RSA WITH SEED CBC SHA *15*
TLS ECDHE RSA WITH 3DES EDE CBC SHA *15*
TLS RSA WITH CAMELLIA 256 CBC SHA *15*
TLS DHE RSA WITH 3DES EDE CBC SHA *16*
TLS DHE RSA WITH AES 128 CBC SHA256 ..... *16*
Support for Emergent Ciphers *16*
Deprecated Ciphers *16*
Prevention of Weak Ciphers *17*
Decryption Bypass Exceptions *17*
Certificate Validation *17*
TLS Session Re-use *17*
Maximum SSL/TLS Handshakes per Second 17
HTTPS Throughput Capacity 18
Appendix: Scorecard 23
Test Methodology 26
Contact Information 26

Table of Figures

Figure 1 – Overall Test Results....2
Figure 2 – TLS ECDHE RSA WITH AES 256 GCM SHA384....8
Figure 3 – TLS ECDHE RSA WITH AES 128 GCM SHA256....9
Figure 4 – TLS ECDHE ECDSA WITH AES 128 GCM SHA256....9
Figure 5 – TLS ECDHE RSA WITH AES 256 CBC SHA384....9
Figure 6 – TLS DHE RSA WITH AES 256 GCM SHA384....10
Figure 7 – TLS ECDHE RSA WITH AES 256 CBC SHA....10
Figure 8 –TLS DHE RSA WITH AES 256 CBC SHA....10
Figure 9 – TLS RSA WITH AES 256 CBC SHA....10
Figure 10 – TLS RSA WITH AES 128 CBC SHA....11
Figure 11 – TLS RSA WITH AES 256 CBC SHA256....11
Figure 12 – TLS RSA WITH AES 256 GCM SHA384....11
Figure 13 – TLS ECDHE RSA WITH AES 128 CBC SHA256....11
Figure 14 – TLS RSA WITH AES 128 CBC SHA256....12
Figure 15 – TLS RSA WITH RC4 128 SHA....12
Figure 16 – TLS RSA WITH AES 128 GCM SHA256....12
Figure 17 – TLS ECDHE RSA WITH AES 128 CBC SHA....12
Figure 18 – TLS ECDHE ECDSA WITH AES 256 GCM SHA384....13
Figure 19 – TLS RSA WITH RC4 128 MD5....13
Figure 20 – TLS ECDHE RSA WITH RC4 128 SHA....13
Figure 21 – TLS DHE RSA WITH AES 128 CBC SHA....13
Figure 22 – TLS DHE RSA WITH AES 128 GCM SHA256....14
Figure 23 – TLS RSA WITH 3DES EDE CBC SHA....14
Figure 24 – TLS DHE RSA WITH AES 256 CBC SHA256....14
Figure 25 – TLS DHE RSA WITH CAMELLIA 256 CBC SHA....14
Figure 26 –TLS DHE RSA WITH SEED CBC SHA....15
Figure 27 – TLS RSA WITH SEED CBC SHA....15
Figure 28 – TLS ECDHE RSA WITH 3DES EDE CBC SHA....15
Figure 29 –TLS RSA WITH CAMELLIA 256 CBC SHA....15
Figure 30 – TLS DHE RSA WITH 3DES EDE CBC SHA....16

Figure 31 – TLS DHE RSA WITH AES 128 CBC SHA256 16
Figure 32 – Maximum HTTP(S) Connections per Second 18
Figure 33 – HTTP Capacity (No Persistence) Single HTTP GET Request (2880 KB) 19
Figure 34 – HTTP Capacity (No Persistence) Single HTTP GET Request (768 KB) 19
Figure 35 – HTTP Capacity (No Persistence) Single HTTP GET Request (192 KB) 20
Figure 36 – HTTP Capacity (No Persistence) Single HTTP GET Request (44 KB) 20
Figure 37 – HTTP Capacity With Persistent Connections with 10 HTTP GET Requests (288 KB) 21
Figure 38 – HTTP Capacity With Persistent Connections with 10 HTTP GET Requests (76.8 KB) 21
Figure 39 – HTTP Capacity With Persistent Connections with 10 HTTP GET Requests (19.2KB) 22
Figure 40 – HTTP Capacity With Persistent Connections with 10 HTTP GET Requests (4.4 KB) 22
Figure 41 – Scorecard 25

SSL/TLS

Use of the Secure Sockets Layer (SSL) protocol and its current iteration, Transport Layer Security (TLS), has risen in accordance with the increasing need for privacy online. Modern cybercampaigns frequently focus on attacking users through the most common web protocols and applications. NSS continues to receive inquiries from enterprise customers during their assessments of vendors that provide SSL/TLS decryption and protection technologies. To this end, NSS tested the capabilities and performance of devices providing SSL/TLS visibility.

SSL/TLS Functionality

Decryption Validation

To confirm that the device under test is correctly decrypting and inspecting SSL/TLS traffic, a validation test was performed prior to functional or performance testing. This test consists of a known exploit embedded in encrypted traffic being passed through the device. NSS has an extensive library of well-known malicious files and exploits suitable for this purpose. Devices were expected to decrypt the stream, detect the exploit, and block the payload. The purpose of this test is not to evaluate the device's security effectiveness, but rather to validate that the device is decrypting and inspecting traffic.

Cipher Selection

To determine the most commonly employed cipher suites for inclusion in testing, ciphers were selected from the 12/31/2017 results of the Alexa Top 1 Million Analysis.[1] The top 30 ciphers from this data were selected for use in functional capability testing and the top four ciphers (representing more than 90% of the distribution) were used for performance testing.

While it is important to understand the scope of real-world cipher usage, it is equally important to keep in mind that not all cipher families are equal in strength or resilience against cryptanalysis and/or side-channel attacks. A review of the top 30 ciphers selected for functional testing indicates a number of deprecated or weak ciphers still in production use around the globe. Whereas some enterprise consumers may continue to require support for deprecated/weak ciphers for legacy systems, NSS supports the recommendations of the Internet Engineering Task Force (IETF) and regulatory frameworks such as the National Institute of Standards and Technology (NIST) with regard to deprecation of ciphers using RC4 (deprecated in RFC 7465[2]) or Triple DES (Special Publication 800-52, Revision 2[3]). As such, while vendors providing SSL/TLS visibility solutions supporting the configuration of deprecated ciphers will receive credit for the flexibility that this provides to consumers, vendors with solutions including a default action to block such ciphers will not be reflected negatively in this report, as NSS considers this the preferred outcome from a security perspective.

[1] Alexa Top 1 Million Analysis performed on 12/31/2017 by Scott Helme; methodology in Appendix A: Cipher Selection Details SSL/TLS Performance Test Methodology v1.3 020218

[2] https://tools.ietf.org/html/rfc7465

[3] https://csrc.nist.gov/CSRC/media/Publications/sp/800-52/rev-2/draft/documents/sp800-52r2-draft.pdf

Cipher Support

The device is expected to be capable of negotiating a wide range of commonly used SSL/TLS ciphers in order to increase the security visibility of potential threats encapsulated in real-world SSL/TLS traffic. This test covered the top 30 cipher suites. Unless otherwise specified, the functional tests used the most common key sizes for RSA (2,048 bit) and ECDSA (256 bit).

Top 30 Cipher Suites from the Alexa Top 1 Million, as of 12/31/2017

- TLS ECDHE RSA WITH AES 256 GCM SHA384
- TLS ECDHE RSA WITH AES 128 GCM SHA256
- TLS ECDHE ECDSA WITH AES 128 GCM SHA256
- TLS ECDHE RSA WITH AES 256 CBC SHA384
- TLS DHE RSA WITH AES 256 GCM SHA384
- TLS ECDHE RSA WITH AES 256 CBC SHA
- TLS DHE RSA WITH AES 256 CBC SHA
- TLS RSA WITH AES 256 CBC SHA
- TLS ECDHE RSA WITH AES 128 CBC SHA
- TLS ECDHE ECDSA WITH AES 256 GCM SHA384
- TLS RSA WITH RC4 128 MD5
- TLS ECDHE RSA WITH RC4 128 SHA
- TLS DHE RSA WITH AES 128 CBC SHA
- TLS DHE RSA WITH AES 128 GCM SHA256
- TLS RSA WITH 3DES EDE CBC SHA
- TLS DHE RSA WITH AES 256 CBC SHA256
- TLS RSA WITH AES 128 CBC SHA
- TLS RSA WITH AES 256 CBC SHA256
- TLS RSA WITH AES 256 GCM SHA384
- TLS ECDHE RSA WITH AES 128 CBC SHA256
- TLS RSA WITH AES 128 CBC SHA256
- TLS RSA WITH RC4 128 SHA
- TLS RSA WITH AES 128 GCM SHA256
- TLS DHE RSA WITH CAMELLIA 256 CBC SHA
- TLS DHE RSA WITH SEED CBC SHA
- TLS RSA WITH SEED CBC SHA
- TLS ECDHE RSA WITH 3DES EDE CBC SHA
- TLS RSA WITH CAMELLIA 256 CBC SHA
- TLS DHE RSA WITH 3DES EDE CBC SHA
- TLS DHE RSA WITH AES 128 CBC SHA256

TLS ECDHE RSA WITH AES 256 GCM SHA384

This cipher was found to be the most widely negotiated of those in the Top 30. Device performance was measured at two different key sizes for this cipher: 2,048 bits and 4,096 bits.

Cipher Rank	1
Cipher Prevalence	41.81%
2,048 bit key size performance	5,832 Mbps
4,096 bit key size performance	5,757 Mbps
Cipher Decrypted	YES
Block Payload	PASS

Figure 2 – TLS ECDHE RSA WITH AES 256 GCM SHA384

TLS ECDHE RSA WITH AES 128 GCM SHA256

This cipher was found to be the second most widely negotiated of those in the Top 30. Device performance was measured at a key size of 2,048 bits.

Cipher Rank	2
Cipher Prevalence	32.44%
2,048 bit key size performance	5,865 Mbps
Cipher Decrypted	YES
Block Payload	PASS

Figure 3 – TLS ECDHE RSA WITH AES 128 GCM SHA256

TLS ECDHE ECDSA WITH AES 128 GCM SHA256

This cipher was found to be the third most widely negotiated of those in the Top 30. Device performance was measured at a key size of 256 bits.

Cipher Rank	3
Cipher Prevalence	12.79%
2,048 bit key size performance	5,970 Mbps
Cipher Decrypted	YES
Block Payload	PASS

Figure 4 – TLS ECDHE ECDSA WITH AES 128 GCM SHA256

TLS ECDHE RSA WITH AES 256 CBC SHA384

This cipher was found to be the fourth most widely negotiated of those in the Top 30. Device performance was measured at a key size of 2,048 bits.

Cipher Rank	4
Cipher Prevalence	4.53%
2,048 bit key size performance	4,048 Mbps
Cipher Decrypted	YES
Block Payload	PASS

Figure 5 – TLS ECDHE RSA WITH AES 256 CBC SHA384

TLS DHE RSA WITH AES 256 GCM SHA384

This cipher was found to be the fifth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	5
Cipher Prevalence	1.49%
Cipher Decrypted	YES
Block Payload	PASS

Figure 6 – TLS DHE RSA WITH AES 256 GCM SHA384

TLS ECDHE RSA WITH AES 256 CBC SHA

This cipher was found to be the sixth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	6
Cipher Prevalence	1.02%
Cipher Decrypted	YES
Block Payload	PASS

Figure 7 – TLS ECDHE RSA WITH AES 256 CBC SHA

TLS DHE RSA WITH AES 256 CBC SHA

This cipher was found to be the seventh most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	7
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 8 –TLS DHE RSA WITH AES 256 CBC SHA

TLS RSA WITH AES 256 CBC SHA

This cipher was found to be the eighth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	8
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 9 – TLS RSA WITH AES 256 CBC SHA

TLS RSA WITH AES 128 CBC SHA

This cipher was found to be the ninth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	9
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 10 – TLS RSA WITH AES 128 CBC SHA

TLS RSA WITH AES 256 CBC SHA256

This cipher was found to be the tenth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	10
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 11 – TLS RSA WITH AES 256 CBC SHA256

TLS RSA WITH AES 256 GCM SHA384

This cipher was found to be the eleventh most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	11
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 12 – TLS RSA WITH AES 256 GCM SHA384

TLS ECDHE RSA WITH AES 128 CBC SHA256

This cipher was found to be the twelfth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	12
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 13 – TLS ECDHE RSA WITH AES 128 CBC SHA256

TLS RSA WITH AES 128 CBC SHA256

This cipher was found to be the thirteenth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	13
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 14 – TLS RSA WITH AES 128 CBC SHA256

TLS RSA WITH RC4 128 SHA

This cipher was found to be the fourteenth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher. The RC4 stream cipher has been deprecated, as of RFC 7465.[2]

Cipher Rank	14
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 15 – TLS RSA WITH RC4 128 SHA

TLS RSA WITH AES 128 GCM SHA256

This cipher was found to be the fifteenth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	15
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 16 – TLS RSA WITH AES 128 GCM SHA256

TLS ECDHE RSA WITH AES 128 CBC SHA

This cipher was found to be the sixteenth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	16
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 17 – TLS ECDHE RSA WITH AES 128 CBC SHA

TLS ECDHE ECDSA WITH AES 256 GCM SHA384

This cipher was found to be the seventeenth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	17
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 18 – TLS ECDHE ECDSA WITH AES 256 GCM SHA384

TLS RSA WITH RC4 128 MD5

This cipher was found to be the eighteenth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher. The RC4 stream cipher has been deprecated, as of RFC 7465.[2]

Cipher Rank	18
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 19 – TLS RSA WITH RC4 128 MD5

TLS ECDHE RSA WITH RC4 128 SHA

This cipher was found to be the nineteenth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher. The RC4 stream cipher has been deprecated, as of RFC 7465.[2]

Cipher Rank	19
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 20 – TLS ECDHE RSA WITH RC4 128 SHA

TLS DHE RSA WITH AES 128 CBC SHA

This cipher was found to be the twentieth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	20
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 21 – TLS DHE RSA WITH AES 128 CBC SHA

TLS DHE RSA WITH AES 128 GCM SHA256

This cipher was found to be the twenty-first most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	21
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 22 – TLS DHE RSA WITH AES 128 GCM SHA256

TLS RSA WITH 3DES EDE CBC SHA

This cipher was found to be the twenty-second most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher. The 3DES cipher has been deprecated by NIST.[3]

Cipher Rank	22
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 23 – TLS RSA WITH 3DES EDE CBC SHA

TLS DHE RSA WITH AES 256 CBC SHA256

This cipher was found to be the twenty-third most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	23
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 24 – TLS DHE RSA WITH AES 256 CBC SHA256

TLS DHE RSA WITH CAMELLIA 256 CBC SHA

This cipher was found to be the twenty-fourth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	24
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 25 – TLS DHE RSA WITH CAMELLIA 256 CBC SHA

TLS DHE RSA WITH SEED CBC SHA

This cipher was found to be the twenty-fifth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	25
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 26 –TLS DHE RSA WITH SEED CBC SHA

TLS RSA WITH SEED CBC SHA

This cipher was found to be the twenty-sixth most widely-negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	26
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 27 – TLS RSA WITH SEED CBC SHA

TLS ECDHE RSA WITH 3DES EDE CBC SHA

This cipher was found to be the twenty-seventh most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher. The 3DES cipher has been deprecated by NIST.[3]

Cipher Rank	27
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 28 – TLS ECDHE RSA WITH 3DES EDE CBC SHA

TLS RSA WITH CAMELLIA 256 CBC SHA

This cipher was found to be the twenty-eighth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	28
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 29 –TLS RSA WITH CAMELLIA 256 CBC SHA

TLS DHE RSA WITH 3DES EDE CBC SHA

This cipher was found to be the twenty-ninth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher. The 3DES cipher has been deprecated by NIST.[3]

Cipher Rank	29
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 30 – TLS DHE RSA WITH 3DES EDE CBC SHA

TLS DHE RSA WITH AES 128 CBC SHA256

This cipher was found to be the thirtieth most widely negotiated of those in the Top 30. The device was not measured for performance using this cipher.

Cipher Rank	30
Cipher Prevalence	<1%
Cipher Decrypted	YES
Block Payload	PASS

Figure 31 – TLS DHE RSA WITH AES 128 CBC SHA256

Support for Emergent Ciphers

In addition to the top 30 ciphers specified previously, support for the following emergent ciphers and parameters was tested:

- TLS ECDHE ECDSA WITH CHACHA20 POLY1305 SHA256
- TLS ECDHE RSA WITH CHACHA20 POLY1305 SHA256
- x25519 Elliptic Curve Key Exchange

While the prevalence of emergent ciphers and elliptic curve parameters continues to rise, in most real-world use cases, equally robust alternate cipher families are included in both client and server preference lists. As such, lack of support for these newer ciphers and parameters in an SSL/TLS visibility solution would almost always be transparent and non-impactful to an enterprise. In that light, while solutions supporting these options will be given full credit, solutions lacking such support will not be negatively reflected in this report.

Deprecated Ciphers

Protection against use of the following deprecated ciphers is an acceptable default option for devices:

- RC4, including the following listed in the Top 30 Cipher Suites above:
    - TLS RSA WITH RC4 128 MD5
    - TLS RSA WITH RC4 128 SHA
    - TLS ECDHE RSA WITH RC4 128 SHA

Prevention of Weak Ciphers

The device is expected to protect against the use of ciphers that are known to offer either weak protection or none at all, including (but not limited to):

- Null ciphers (no encryption of data provided)
- Anonymous ciphers (no authentication provided)

Protection against use of the following ciphers is also an acceptable default option for devices:

- Triple DES (3DES or TDEA), including the following listed in the Top 30 Cipher Suites above:
    - TLS RSA WITH 3DES EDE CBC SHA
    - TLS ECDHE RSA WITH 3DES EDE CBC SHA
    - TLS DHE RSA WITH 3DES EDE CBC SHA

Decryption Bypass Exceptions

The device is expected to support the configuration of policies that permit conditional bypass of decryption in order to preserve privacy, either for regulatory or other reasons. The device must maintain decryption capabilities as tested in the *Cipher Support* section concurrently with these conditional bypass rules; i.e., turning off all decryption on the device is not an acceptable method for meeting requirements in this section. The device was tested for decryption bypass capabilities under various conditions, including:

- Layer 3 information (i.e., bypass based on source or destination IP address)
- Layer 4 information (i.e., bypass based on TCP port number)
- Server Name Indication (SNI) TLS extension information
- Site category based on Common Name (CN) and/or Subject Alternative Name (SAN)

Certificate Validation

The device is expected to validate the status of all SSL/TLS certificates presented, except in cases where decryption bypass is enabled. When presented with an invalid certificate, the device must either prevent the establishment of a connection or replicate the original invalid status in the proxied/resigned certificate presented to the client, such that the client is aware of the potential risk.

TLS Session Re-use

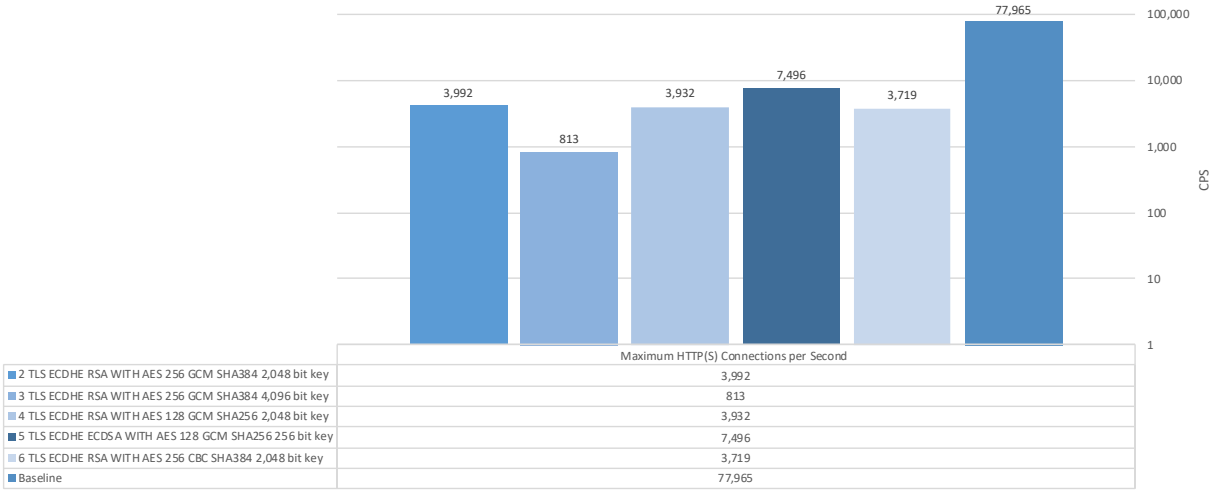
In order to improve performance and reduce the overhead associated with conducting the full handshake for each session, the TLS protocol allows for abbreviated handshakes, which re-use previously established sessions. The two primary methods for session re-use are session IDs and session tickets. Whereas session IDs are included in the main TLS specification, session tickets are an extension of the specification, detailed in a separate RFC. Support for both of these methods is tested in this section.

These tests assess the scope of support for a wide range of cipher suites, including functional checks for common extensions to the TLS protocol, as well as policies to bypass the decryption process for certain subsets of traffic.

Maximum SSL/TLS Handshakes per Second

This test is designed to determine the maximum HTTPS connection rate of the device with a one-byte response size. This type of traffic is atypical of a normal network, but the negligible payload size provides a means to

measure the device's SSL/TLS handshake performance independent of throughput performance. An increasing number of new sessions is established through the device until a maximum is reached and each session is immediately closed upon successful negotiation of the SSL/TLS handshake and transfer of the payload.



	Maximum HTTP(S) Connections per Second
2 TLS ECDHE RSA WITH AES 256 GCM SHA384 2,048 bit key	3,992
3 TLS ECDHE RSA WITH AES 256 GCM SHA384 4,096 bit key	813
4 TLS ECDHE RSA WITH AES 128 GCM SHA256 2,048 bit key	3,932
5 TLS ECDHE ECDSA WITH AES 128 GCM SHA256 256 bit key	7,496
6 TLS ECDHE RSA WITH AES 256 CBC SHA384 2,048 bit key	3,719
Baseline	77,965

Figure 32 – Maximum HTTP(S) Connections per Second

HTTPS Throughput Capacity

The aim of these tests is to stress the HTTPS engine and determine how the device copes with network loads of varying average packet size and varying connections per second. By creating session-based traffic with varying session lengths, the device is forced to track valid TCP sessions, thus ensuring a higher workload than for simple packet-based background traffic. This provides a test environment that is as close to real-world conditions as it is possible to achieve in a lab environment, while ensuring accuracy and repeatability. Each transaction consists of either a single (1) HTTP(S) GET request or ten (10) HTTP(S) GETs and there are no transaction delays (i.e., the web server responds immediately to all requests). All packets contain valid payload (a mix of binary and ASCII objects) and address data, and this test provides a feasible representation of a live network (albeit one biased toward HTTPS traffic) at various network loads.

Figure 33 through Figure 40 depict the results of the HTTPS Throughput Capacity tests.

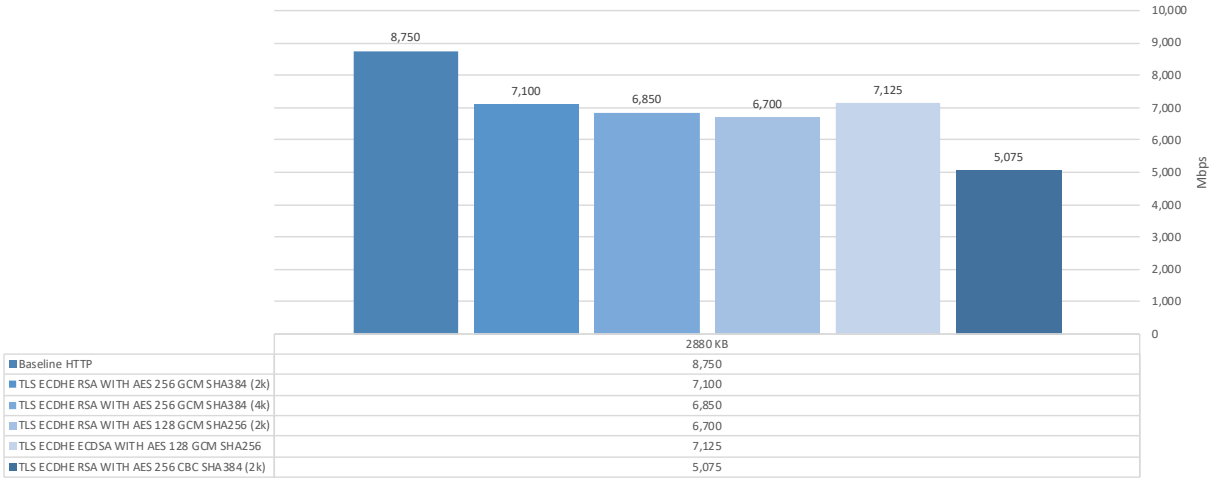


Figure 33 – HTTP Capacity (No Persistence) Single HTTP GET Request (2880 KB)

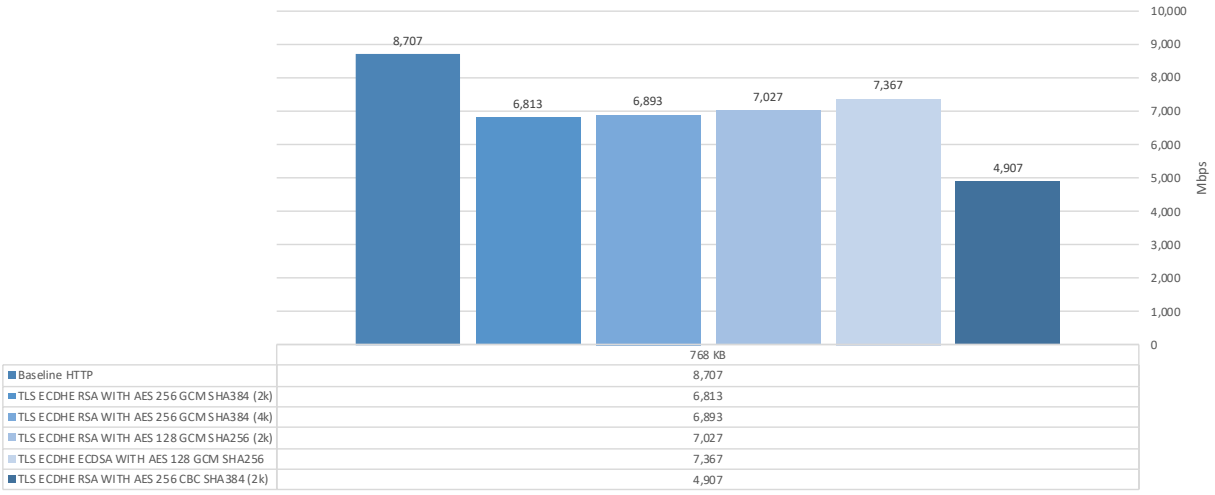
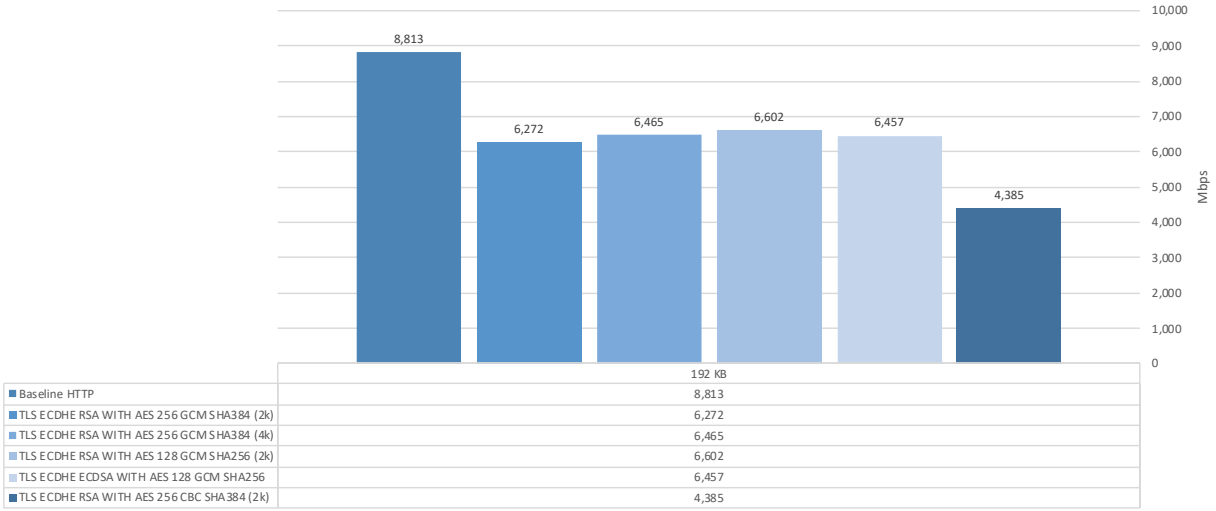
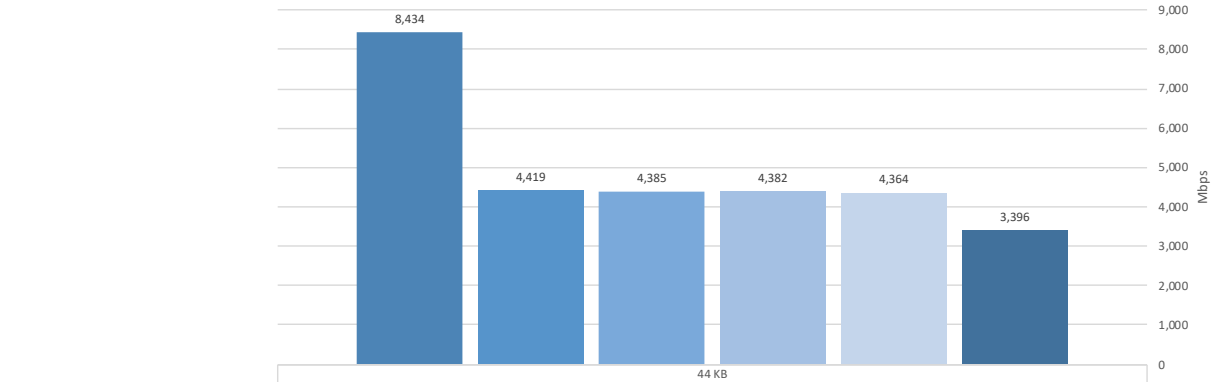


Figure 34 – HTTP Capacity (No Persistence) Single HTTP GET Request (768 KB)



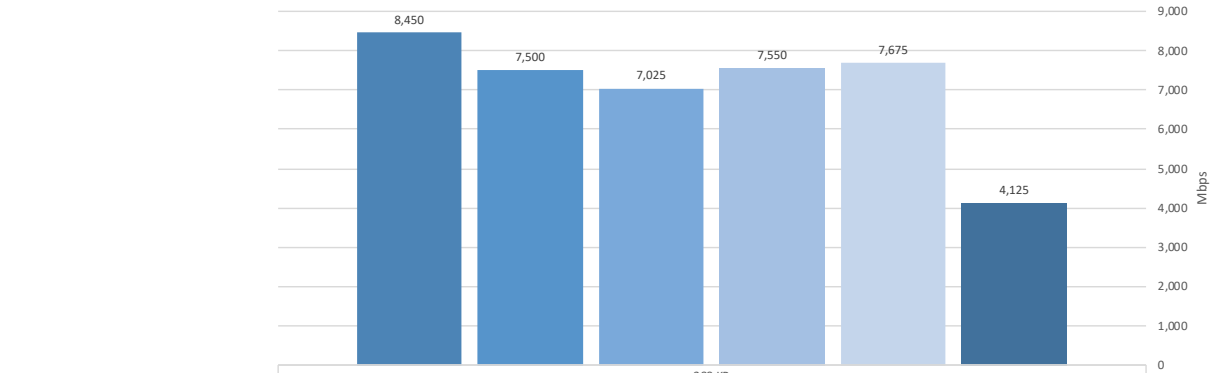
	192 KB
Baseline HTTP	8,813
TLS ECDHE RSA WITH AES 256 GCM SHA384 (2k)	6,272
TLS ECDHE RSA WITH AES 256 GCM SHA384 (4k)	6,465
TLS ECDHE RSA WITH AES 128 GCM SHA256 (2k)	6,602
TLS ECDHE ECDSA WITH AES 128 GCM SHA256	6,457
TLS ECDHE RSA WITH AES 256 CBC SHA384 (2k)	4,385

Figure 35 – HTTP Capacity (No Persistence) Single HTTP GET Request (192 KB)



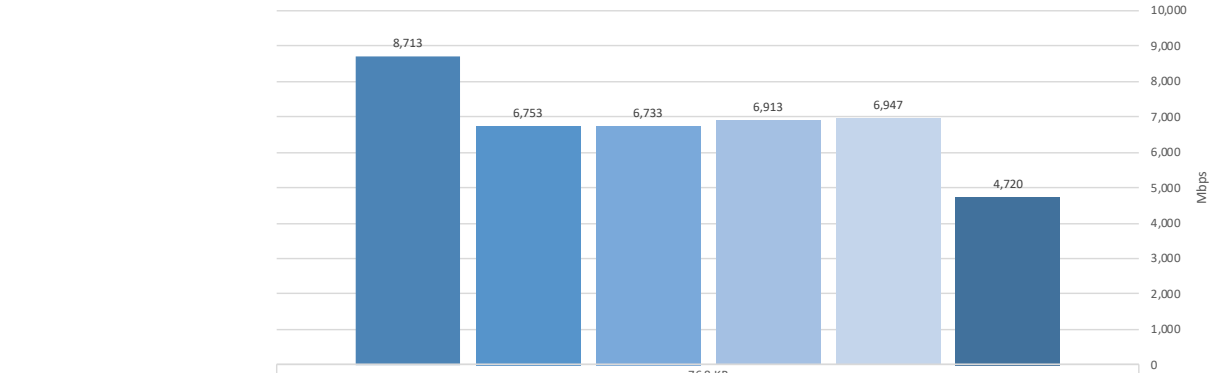
	44 KB
Baseline HTTP	8,434
TLS ECDHE RSA WITH AES 256 GCM SHA384 (2k)	4,419
TLS ECDHE RSA WITH AES 256 GCM SHA384 (4k)	4,385
TLS ECDHE RSA WITH AES 128 GCM SHA256 (2k)	4,382
TLS ECDHE ECDSA WITH AES 128 GCM SHA256	4,364
TLS ECDHE RSA WITH AES 256 CBC SHA384 (2k)	3,396

Figure 36 – HTTP Capacity (No Persistence) Single HTTP GET Request (44 KB)



	288 KB
Baseline HTTP	8,450
TLS ECDHE RSA WITH AES 256 GCM SHA384 (2k)	7,500
TLS ECDHE RSA WITH AES 256 GCM SHA384 (4k)	7,025
TLS ECDHE RSA WITH AES 128 GCM SHA256 (2k)	7,550
TLS ECDHE ECDSA WITH AES 128 GCM SHA256	7,675
TLS ECDHE RSA WITH AES 256 CBC SHA384 (2k)	4,125

Figure 37 – HTTP Capacity With Persistent Connections with 10 HTTP GET Requests (288 KB)



	76.8 KB
Baseline HTTP	8,713
TLS ECDHE RSA WITH AES 256 GCM SHA384 (2k)	6,753
TLS ECDHE RSA WITH AES 256 GCM SHA384 (4k)	6,733
TLS ECDHE RSA WITH AES 128 GCM SHA256 (2k)	6,913
TLS ECDHE ECDSA WITH AES 128 GCM SHA256	6,947
TLS ECDHE RSA WITH AES 256 CBC SHA384 (2k)	4,720

Figure 38 – HTTP Capacity With Persistent Connections with 10 HTTP GET Requests (76.8 KB)

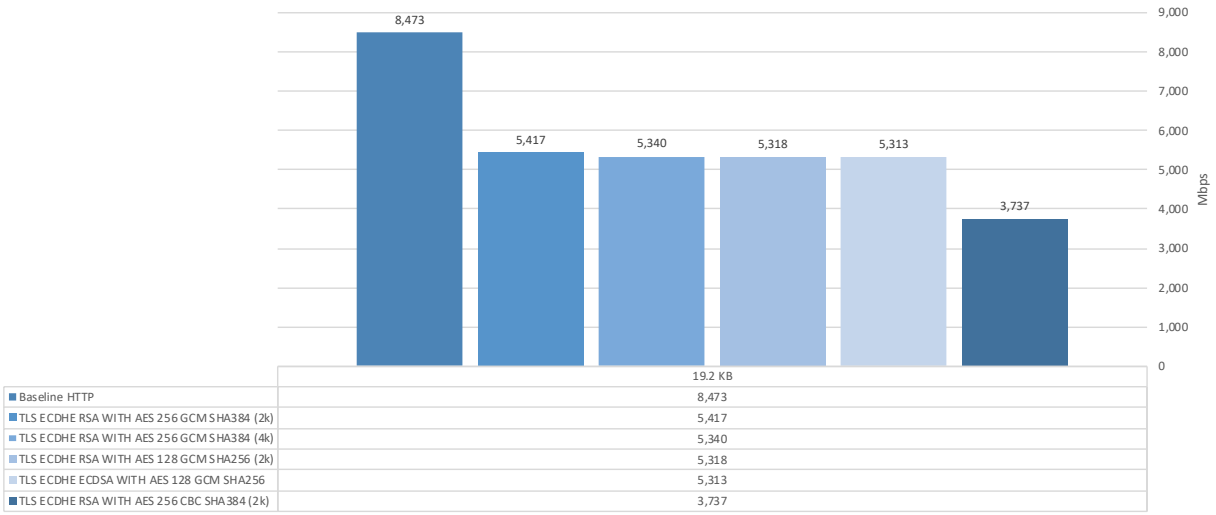


Figure 39 – HTTP Capacity With Persistent Connections with 10 HTTP GET Requests (19.2KB)

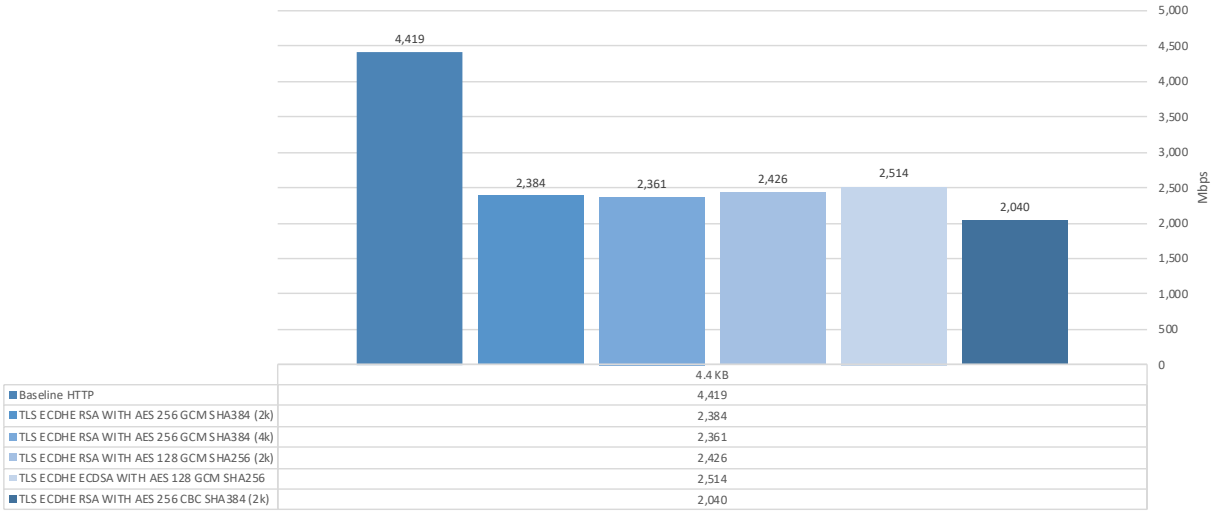


Figure 40 – HTTP Capacity With Persistent Connections with 10 HTTP GET Requests (4.4 KB)

Appendix: Scorecard

Description	Result	
SSL/ TLS Functionality Testing	Decryption	
TLS ECDHE RSA WITH AES 256 GCM SHA384	YES	
TLS ECDHE RSA WITH AES 128 GCM SHA256	YES	
TLS ECDHE ECDSA WITH AES 128 GCM SHA256	YES	
TLS ECDHE RSA WITH AES 256 CBC SHA384	YES	
TLS DHE RSA WITH AES 256 GCM SHA384	YES	
TLS ECDHE RSA WITH AES 256 CBC SHA	YES	
TLS DHE RSA WITH AES 256 CBC SHA	YES	
TLS RSA WITH AES 256 CBC SHA	YES	
TLS RSA WITH AES 128 CBC SHA	YES	
TLS RSA WITH AES 256 CBC SHA256	YES	
TLS RSA WITH AES 256 GCM SHA384	YES	
TLS ECDHE RSA WITH AES 128 CBC SHA256	YES	
TLS RSA WITH AES 128 CBC SHA256	YES	
TLS RSA WITH RC4 128 SHA	YES	
TLS RSA WITH AES 128 GCM SHA256	YES	
TLS ECDHE RSA WITH AES 128 CBC SHA	YES	
TLS ECDHE ECDSA WITH AES 256 GCM SHA384	YES	
TLS RSA WITH RC4 128 MD5	YES	
TLS ECDHE RSA WITH RC4 128 SHA	YES	
TLS DHE RSA WITH AES 128 CBC SHA	YES	
TLS DHE RSA WITH AES 128 GCM SHA256	YES	
TLS RSA WITH 3DES EDE CBC SHA	YES	
TLS DHE RSA WITH AES 256 CBC SHA256	YES	
TLS DHE RSA WITH CAMELLIA 256 CBC SHA	YES	
TLS DHE RSA WITH SEED CBC SHA	YES	
TLS RSA WITH SEED CBC SHA	YES	
TLS ECDHE RSA WITH 3DES EDE CBC SHA	YES	
TLS RSA WITH CAMELLIA 256 CBC SHA	YES	
TLS DHE RSA WITH 3DES EDE CBC SHA	YES	
TLS DHE RSA WITH AES 128 CBC SHA256	YES	
Performance		
Maximum HTTP(S) Connections per Second	Key Size	CPS
TLS ECDHE RSA WITH AES 256 GCM SHA384	2,048 bit key	3,992
TLS ECDHE RSA WITH AES 256 GCM SHA384	4,096 bit key	813
TLS ECDHE RSA WITH AES 128 GCM SHA256	2,048 bit key	3,932
TLS ECDHE ECDSA WITH AES 128 GCM SHA256	256 bit key	7,496
TLS ECDHE RSA WITH AES 256 CBC SHA384	2,048 bit key	3,719

No Encryption (Baseline)	Session	Response Size	CPS	Mbps
HTTP Capacity, No Persistence	Single HTTP GET Request	2880 KB	350	8,750
		768 KB	1306	8,707
		192 KB	5288	8,813
		44 KB	21,086	8,434
HTTP Capacity With Persistent Connections	10 HTTP GET Requests	288 KB	338	8,450
		76.8 KB	1,307	8,713
		19.2 KB	5,084	8,473
		4.4 KB	11,048	4,419
TLS ECDHE RSA WITH AES 256 GCM SHA384 (2k)	Session	Response Size	CPS*	Mbps
HTTP Capacity, No Persistence	Single HTTPS GET Request	2880 KB	284	7,100
		768 KB	1,022	6,813
		192 KB	3,763	6,272
		44 KB	11,047	4,419
HTTP Capacity With Persistent Connections	10 HTTPS GET Requests	288 KB	300	7,500
		76.8 KB	1,013	6,753
		19.2 KB	3,250	5,417
		4.4 KB	5,961	2,384
TLS ECDHE RSA WITH AES 256 GCM SHA384 (4k)	Session	Response Size	CPS*	Mbps
HTTP Capacity, No Persistence	Single HTTPS GET Request	2880 KB	274	6,850
		768 KB	1,034	6,893
		192 KB	3,879	6,465
		44 KB	10,963	4,385
HTTP Capacity With Persistent Connections	10 HTTPS GET Requests	288 KB	281	7,025
		76.8 KB	1,010	6,733
		19.2 KB	3,204	5,340
		4.4 KB	5,902	2,361
TLS ECDHE RSA WITH AES 128 GCM SHA256 (2k)	Session	Response Size	CPS*	Mbps
HTTP Capacity, No Persistence	Single HTTPS GET Request	2880 KB	268	6,700
		768 KB	1,054	7,027
		192 KB	3,961	6,602
		44 KB	10,956	4,382
HTTP Capacity With Persistent Connections	10 HTTPS GET Requests	288 KB	302	7,550
		76.8 KB	1,037	6,913
		19.2 KB	3,191	5,318
		4.4 KB	6,065	2,426

TLS ECDHE ECDSA WITH AES 128 GCM SHA256	Session	Response Size	CPS*	Mbps
HTTP Capacity, No Persistence	Single HTTPS GET Request	2880 KB	285	7,125
		768 KB	1,105	7,367
		192 KB	3,874	6,457
		44 KB	10,911	4,364
HTTP Capacity With Persistent Connections	10 HTTPS GET Requests	288 KB	307	7,675
		76.8 KB	1,042	6,947
		19.2 KB	3,188	5,313
		4.4 KB	6,285	2,514
TLS ECDHE RSA WITH AES 256 CBC SHA384 (2k)	Session	Response Size	CPS*	Mbps
HTTP Capacity, No Persistence	Single HTTPS GET Request	2880 KB	203	5,075
		768 KB	736	4,907
		192 KB	2,631	4,385
		44 KB	8,491	3,396
HTTP Capacity With Persistent Connections	10 HTTPS GET Requests	288 KB	165	4,125
		76.8 KB	708	4,720
		19.2 KB	2,242	3,737
		4.4 KB	5,099	2,040

Figure 41 – Scorecard

* Weighted average of the SSL/TLS traffic that NSS expects an NGFW to experience in an enterprise environment.

Test Methodology

NSS Labs SSL/TLS Performance Test Methodology v1.3

A copy of the test methodology is available at www.nsslabs.com.

Contact Information

NSS Labs, Inc.
3711 South MoPac Expressway
Suite 400
Austin, TX 78735 USA
info@nsslabs.com
www.nsslabs.com

This and other related documents are available at: **www.nsslabs.com**. To receive a licensed copy or report misuse, please contact NSS Labs.

© 2018 NSS Labs, Inc. All rights reserved. No part of this publication may be reproduced, copied/scanned, stored on a retrieval system, e-mailed or otherwise disseminated or transmitted without the express written consent of NSS Labs, Inc. ("us" or "we").

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. "You" or "your" means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.

2. The information in this report is believed by us to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.

3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.

5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.

6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.