The Importance of Broad Cipher Suite Support When Inspecting Encrypted Traffic

A primer on the critical role that cipher suites play in the inspection of SSL encrypted traffic

WHITE PAPER

Symantec

Introduction

Inspecting SSL/TLS has become crucial for an increasingly large percentage of enterprise security teams. It's predicted that 75% of internet traffic will be encrypted within two years.[1] Consequently, it's critical that enterprises have the ability to decrypt this traffic, make it temporarily visible, and hand it to security inspection engines like Symantec DLP, for the prevention of data exfiltration and compliance violations, and Symantec Content Analysis, which prevents attacks and blocks advanced threats.

Not surprisingly, as SSL traffic inspection has become a key capability for network security products, the market has seen a rise in the number of security vendors making inaccurate and unsubstantiated claims regarding their ability to perform secure SSL traffic inspection. Unfortunately, general claims and vague detail make it increasingly difficult for enterprises to select solutions that provide comprehensive, high-security inspection capabilities without the downside of exposing the enterprise to new security risk. This most commonly occurs when vendors lack support for the latest cipher suites and force a downgrade to a weaker cipher when traffic needs to be re-encrypted after inspection or, worse yet, simply pass traffic through without inspection ever occurring.

Organizations need not accept the security tradeoff that some SSL visibility vendors make behind the scenes. In this document, we'll examine what's at risk and how you can spot potentially avoidable security compromises to your information.

You can use this step-by-step guide to validate the cipher suite coverage of your current SSL inspection solution. Once you determine what, if any, security tradeoffs are being made, you can evaluate alternatives in the market to improve your security posture and ensure you are prepared to prevent threats and enforce information security policies in an increasingly encrypted world.

Implications of Broad Cipher Suite Support

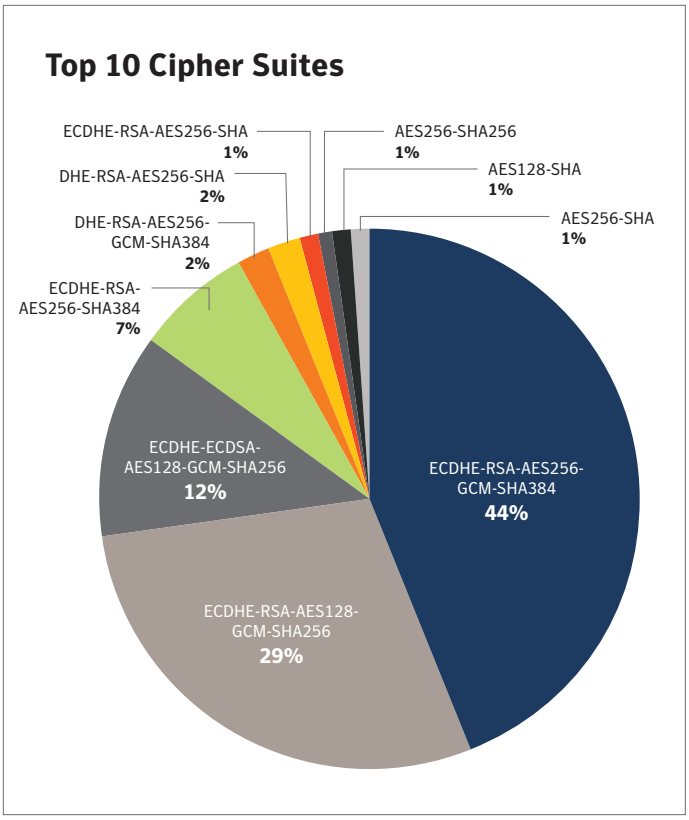
When an SSL session is established, a client device shares the set of cipher suites that it supports with the server. The client's set is rank-ordered giving highest preference to the most secure ciphers. The server then negotiates and selects a specific cipher suite to use in the communication. If the server is not prepared to use any of the cipher suites advertised by the client, then it will not allow the session.

When an SSL inspection device is deployed between a client and a server using encryption, the middle device needs to broker an agreement with each side. SSL inspection devices typically establish a separate communication channel on each side for encrypted traffic. The data in between is decrypted and can be scanned for malware. This is where a typical DLP, IPS, and sandbox solution resides.

In an ideal situation, the SSL inspection product supports the same cipher suites used by the client and server. If the SSL inspection product does not support the same cipher as either the client or the server, it negotiates a different cipher suite that is acceptable by the other side. This process is known as a downgrade of the cipher suite and should be avoided since it leads to a degradation of the security posture of the enterprise. **Logic dictates that an SSL inspection product that supports more cipher suites would lessen the chance of cipher degradation and offer a higher level of security and protection.**

According to a recent study[2] examining Alexa's top 1 million websites using encryption, over 92.8% prefer to use ECDHE based ciphers. Given its broad use, you need to understand what will happen to SSL security if this cipher suite is not supported by your inspection solution. Organizations looking to implement an SSL inspection solution should determine the minimum level of cipher suite support they require. If the SSL inspection solution you're evaluating does not support the preferred ciphers of a website, you may either need to block access to that site (poor user experience) or choose not to intercept at all (poor security). Worse yet, some solutions may choose on their own to bypass inspection if an appropriate cipher suite cannot be identified during the exchange. Consequently, poor support for the preferred suites can compromise the security posture of the organization using inadequate solutions.

[1] https://www.nsslabs.com/company/news/press-releases/nss-labs-predicts-75-of-web-traffic-will-be-encrypted-by-2019
[2] https://scotthelme.co.uk/alexa-top-1-million-analysis-feb-2017



Validating the Cipher Suites Your Solution Supports

Google and Qualys provide unique free websites that can be used to test and confirm cipher suite support. Each validates whether a deployed solution will negotiate the most secure cipher for the communication between the client and server. You can access the sites with these links:

Google: https://cert-test.sandbox.google.com
Qualys: https://www.ssllabs.com/ssltest

The following section provides step by step instructions to display the supported cipher suites for any SSL inspection solution using each site. We recommend you run your own tests and, to validate afterward, re-run it with a different web browser than you used in your initial testing. There may be slight variations but the final results should be the same.

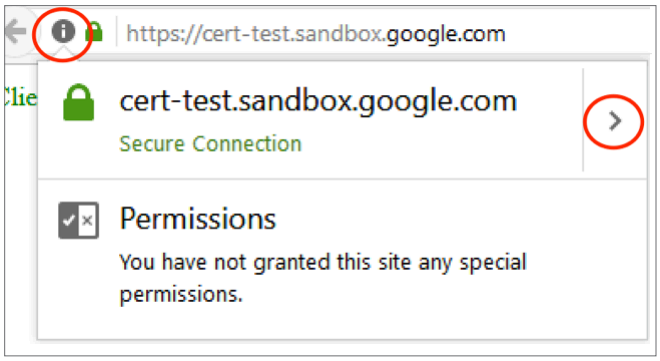
Google Test

Establish a benchmark by accessing Google site without SSL inspection.

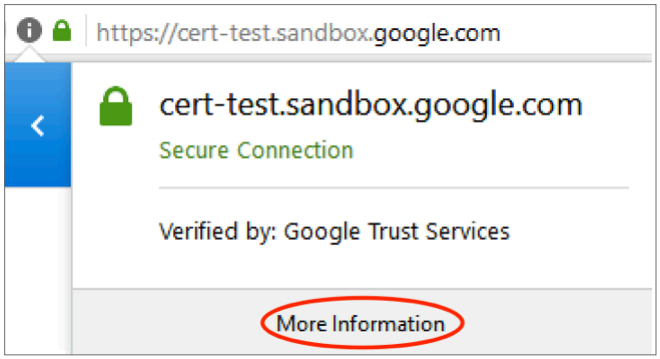
The first step in determining if an inspection solution is adhering to a specific browser's security preferences is to directly connect to the server without an inspection solution in the middle. This allows you to determine the natural cipher suite selection that occurs without an inspection tool in place. We are showing the steps using a Firefox browser, but similar steps can be shown with other popular browsers such as Explorer and Chrome.

1. Access https://cert-test.sandbox.google.com, "Client test successful" message will be displayed.

2. Click on the "i" icon, then the right-arrow icon ">".



3. Click on "More Information" to display the certificate details shown in Figure 1 (next page).



Direct access to the Google site, with no SSL inspection device in between, shows site preference for highly-secure TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys.

This benchmark will be a point of comparison for testing your SSL Intercept tool.

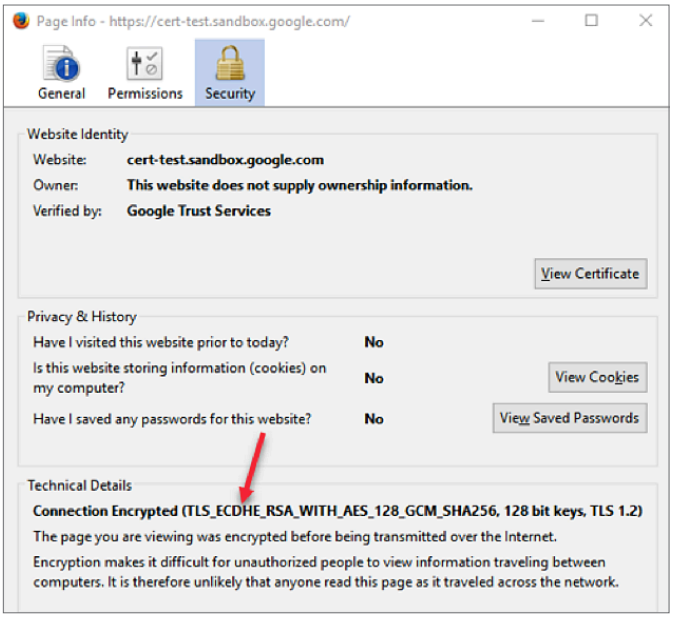


Figure 1: Going to the Goggle website directly with a Firefox browser shows the ideal Cipher Suite negotiated between Client and Server.

Access Google Site with SSL Inspection Tool in Place

Next, go to the Google site with your tool in between conducting SSL inspection. Repeat steps 1–3 from the baseline exercise. You'll then want to compare certificate details against the benchmark you've created.

For this site, the SSL inspection solution was unable to handle the desired ECDHE key exchange and negotiated to a less secure cipher. Note that this session uses RSA for key exchange, meaning it is vulnerable to a type of attack known as a replay attack. Also, note that the SHA hashing function is being used to sign, and SHA is now deprecated.[3]

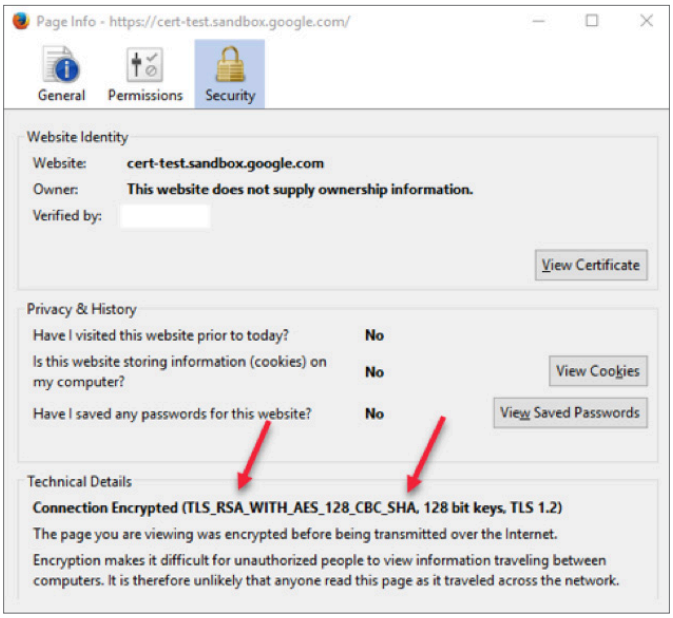


Figure 2: Here the Google site is accessed by the same browser going through a different SSL inspection solution and displaying a cipher negotiated to use TLS_RSA_WITH_AES_128_CBC_SHA, 128 bit keys. This selection weakens the security of the session and introduces vulnerability.

Now Compare Your Results to Symantec ProxySG or Web Security Service with SSI Inspection Enabled

Having an extensive list of highly secure Cipher Suites is important. Symantec ProxySG and Web Security Service provide a large selection of 39 native cipher suites including important ciphers needed for high security SSL/TLS interception. That enables a comparative advantage over competitors that enable far fewer within their native selection. Consequently, ProxySG and Web Security Service are able to support the cipher preferred by client and server and not force a downgrade to another further down on the accepted list. As you determine how many high security ciphers you need while evaluating an SSL Inspection solution use the Symantec list as a point of comparison.

Most SSL Inspection products list them on their websites as well, and are easily found via search engines.

Figure 3 shows the same Google site accessed through a Symantec Blue Coat ProxySG and Web Security Service.

[3] https://www.symantec.com/theme/sha2-transition

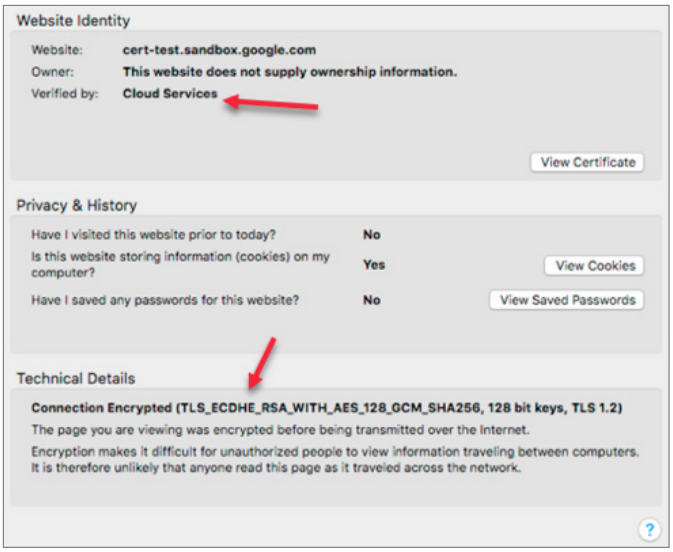


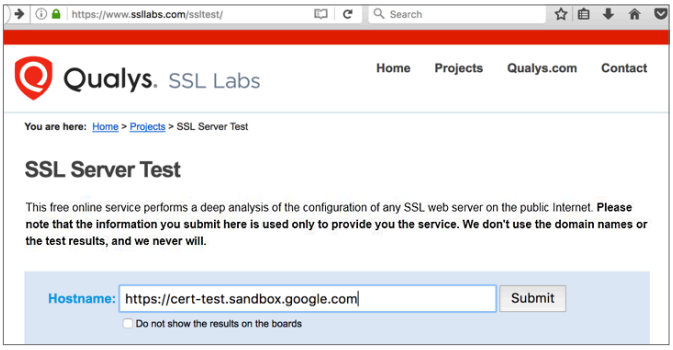
Figure 3: Accessing the Google site through Symantec ProxySG and Web Security Service allows for the use of the recommended ECDHE key exchange and that no forced cipher downgrade is required. Just like our benchmark, ProxySG and Web Security Service both use the preferred cipher of TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys.

Qualys SSL Labs Server Testing

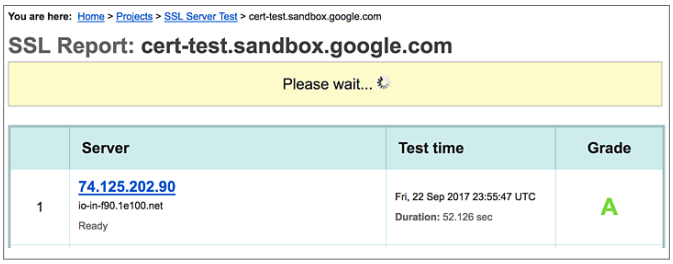
Qualys also provides a free online service at https://www.ssllabs.com/ssltest. This test performs a deep analysis of the configuration of any SSL web server on the public internet. Among the rich detail it provides is a list of ciphers supported by the server.

To conduct your own test, follow the simple step outlined below as we've done with ProxySG and Web Security Service.

1. Access https://www.ssllabs.com/ssltest via Firefox.
2. Enter https://cert-test.sandbox.google.com and click submit.



3. Click on "74.125.202.90" after analysis is completed displaying a grade.



4. Scroll down to "Configuration > Cipher Suites" to display the Cipher Suites list shown in Figure 4.

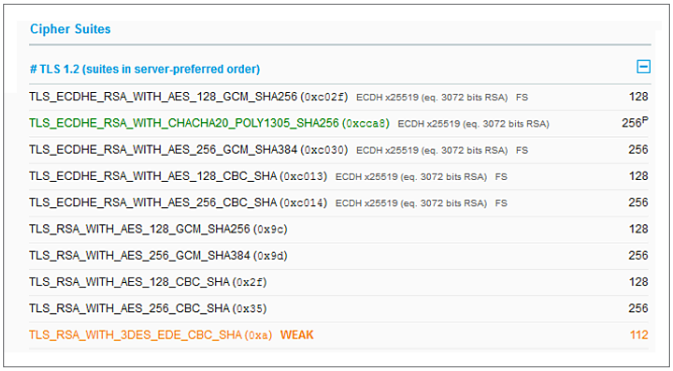


Figure 4: Cipher Preferred Order for cert-test.sandbox.google.com

This test is valuable in showing the rank order of suites offered by the client to the server, routed through an inspection tool. Here we see a preference for the ECHDE key exchange, this enables *Perfect Forward Secrecy*, a method that does not have the vulnerability to the type of replay attack that other solutions could introduce if a highly secure cipher suite is not supported. It also maintains the SHA256, avoiding the signature deprecation that could exist in other SSL inspection solutions due to lack of support.

Run the test on your own and then re-run it from a different browser. Hopefully your results demonstrate a similar level of coverage and preference and strong crypto support.

Why Your Results Matter

In March 2017, the Computer Emergency Response Team (US-CERT) issued an advisory on the potential dangers of inspecting HTTPS traffic because it became aware that many products weaken the security of the connection between the user device and the server.[4]

A primary source for the US-CERT's alert was an academic research study[5] that explored the issue after evaluating a number of solutions.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | C³ VP

Alert (TA17-075A)
HTTPS Interception Weakens TLS Security

More Alerts

Original release date: March 16, 2017

Print | Tweet | Send | Share

Systems Affected

All systems behind a hypertext transfer protocol secure (HTTPS) interception product are potentially affected.

Overview

Many organizations use HTTPS interception products for several purposes, including detecting malware that uses HTTPS connections to malicious servers. The CERT Coordination Center (CERT/CC) explored the tradeoffs of using HTTPS interception in a blog post called The Risks of SSL Inspection [1].

Organizations that have performed a risk assessment and determined that HTTPS inspection is a requirement should ensure their HTTPS inspection products are performing correct transport layer security (TLS) certificate validation. Products that do not properly ensure secure TLS communications and do not convey error messages to the user may further weaken the end-to-end protections that HTTPS aims to provide.

Description

TLS and its predecessor, Secure Sockets Layer (SSL), are important Internet protocols that encrypt communications over the Internet between the client and server. These protocols (and protocols that make use of TLS and SSL, such as HTTPS) use certificates to establish an identity chain showing that the connection is with a legitimate server verified by a trusted third-party certificate authority.

HTTPS inspection works by intercepting the HTTPS network traffic and performing a man-in-the-middle (MiTM) attack on the connection. In MiTM attacks, sensitive client data can be transmitted to a malicious party spoofing the intended server. In order to perform HTTPS inspection without presenting client warnings, administrators must install trusted certificates on client devices. Browsers and other client applications use this certificate to validate encrypted connections created by the HTTPS inspection product. In addition to the problem of not being able to verify a web server's certificate, the protocols and ciphers that an HTTPS inspection product negotiates with web servers may also be invisible to a client. The problem with this architecture is that the client systems have no way of independently validating the HTTPS connection. The client can only verify the connection between itself and the HTTPS interception product. Clients must rely on

In this study, Blue Coat/Symantec received an "A" in our management of encrypted traffic while every single other vendor received a "C" or "F." If your solution was not tested or declined to participate in the study, we suggest evaluating against the same four criteria used by the researchers.

ProxySG received an A grade based on top scores in these four test categories.

1. Supported the latest TLS version
2. **A strong set of ciphers that mirror the browser**
3. Proper validation of certificates
4. Not showing vulnerability to testing for known TLS attacks

Product	Grade	Validates Certificates	Modern Ciphers	Advertises RC4	TLS Version	Grading Notes
A10 vThunder SSL Insight	F	✓	✓	Yes	1.2	Advertises export ciphers
Blue Coat ProxySG 6642	A*	✓	✓	No	1.2	Mirrors client ciphers
Barracuda 610Vx Web Filter	C	✓	×	Yes	1.0	Vulnerable to Logjam attack
Checkpoint Threat Prevention	F	✓	×	Yes	1.0	Allows expired certificates
Cisco IronPort Web Security	F	✓	✓	Yes	1.2	Advertises export ciphers
Forcepoint TRITON AP-WEB Cloud	C	✓	✓	No	1.2	Accepts RC4 ciphers
Fortinet FortiGate 5.4.0	C	✓	✓	No	1.2	Vulnerable to Logjam attack
Juniper SRX Forward SSL Proxy	C	✓	×	Yes	1.2	Advertises RC4 ciphers
Microsoft Threat Mgmt. Gateway	F	×	×	Yes	SSLv2	No certificate validation
Sophos SSL Inspection	C	✓	✓	Yes	1.2	Advertises RC4 ciphers
Untangle NG Firewall	C	✓	×	Yes	1.2	Advertises RC4 ciphers
WebTitan Gateway	F	×	✓	Yes	1.2	Broken certificate validation

Fig. 3: **Security of TLS Interception Middleboxes**—We evaluate popular network middleboxes that act as TLS interception proxies. We find that nearly all reduce connection security and five introduce severe vulnerabilities. *Mirrors browser ciphers.

Next Steps

While inspecting SSL provides invaluable insight for finding potential threats traversing the network, it should not introduce new vulnerabilities that can be exploited by cyber-criminals. Fortunately, some products allow you to inspect SSL traffic without compromising security. Spend time to determine if your SSL inspection solution follows industry best practices for secure HTTPS interception. You'll want to know that your solution supports broad coverage of today's high-security cipher suites and is prepared to keep pace with industry change, especially with the forecasted rate of growth of encrypted traffic over the next 5 years.

For the strongest security posture, ensure that your SSL Inspection solution is respecting the Cipher Suite ordering requested by the browser. Finally, trust but verify. Run these test on your own and see the results. If you're not satisfied with what you see, Symantec is here to help.

[4] https://www.us-cert.gov/ncas/alerts/TA17-075A
[5] https://jhalderm.com/pub/papers/interception-ndss17.pdf

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™
350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

SYMC_wp_Broad_Cipher_Suite Support_EN_v1g.indd