BIG-IP SSL Cipher History

David Holmes, 2015-06-05

John Hall, the fuzz-master at F5, put together this handy spreadsheet showing the SSL cipher suite support sets for F5 BIG-IP software releases over the years.

At the time of this writing, most BIG-IPs in the wild are somewhere between 11.2 and 11.4. But there are, and probably will always be, customers running versions as old as 10.2.4.

The green arrows indicate support in the NATIVE SSL stack. The NATIVE stack is F5's custom SSL code. Most of the ciphers are offloaded to hardware when acceleration is available. Though some of them, such as the GCM suites, are only handled in software at this time.

The red arrows indicate support in the COMPAT stack. The COMPAT stack pulls in the OpenSSL processing code. Typically this is only used for legacy clients that can only talk to OpenSSL. These are few and far between and thus the COMPAT stack is very rarely seen in the wild (less than 1%).

Anyway, this is a handy eye-chart for research or provisioning for BIG-IP and SSL.

Max of String	ADH-AES128-GCM-SHA256	ADH-AES128-SHA	ADH-AES256-GCM-SHA384	ADH-AES256-SHA	ADH-DES-CBC3-SHA	ADH-DES-CBC-SHA	ADH-RC4-MD5	AES128-GCM-SHA256	AES128-SHA	AES128-SHA256	AES256-GCM-SHA384	AES256-SHA	AES256-SHA256	CAMELLIA128-SHA	CAMELLIA256-SHA	DES-CBC3-SHA	DES-CBC-SHA	DHE-DSS-AES128-GCM-SHA256	DHE-DSS-AES128-SHA
BIG-IP v10.2.1		▼		▼	▼	▼	▼		▲			▲				▲	▲		
BIG-IP v10.2.2		▼		▼	▼	▼	▼		▲			▲				▲	▲		
BIG-IP v10.2.3		▼		▼	▼	▼	▼		▲	▲		▲	▲			▲	▲		
BIG-IP v10.2.4		▼		▼	▼	▼	▼		▲	▲		▲	▲			▲	▲		
BIG-IP v11.0.0		▼		▼	▼	▼	▼		▲	▲		▲	▲			▲	▲		
BIG-IP v11.1.0		▼		▼	▼	▼	▼		▲	▲		▲	▲			▲	▲		
BIG-IP v11.2.0		▼		▼	▼	▼	▼		▲	▲		▲	▲			▲	▲		
BIG-IP v11.2.1		▼		▼	▼	▼	▼		▲	▲		▲	▲			▲	▲		
BIG-IP v11.3.0		▼		▼	▼	▼	▼		▲	▲		▲	▲			▲	▲		
BIG-IP v11.4.0		▼		▼	▼	▼	▼		▲	▲		▲	▲			▲	▲		
BIG-IP v11.4.1		▼		▼	▼	▼	▼		▲	▲		▲	▲			▲	▲		
BIG-IP v11.5.0	▲	▼	▲	▼	▼	▼	▼	▲	▲	▲	▲	▲	▲			▲	▲	▲	▲
BIG-IP v11.5.1	▲	▼	▲	▼	▼	▼	▼	▲	▲	▲	▲	▲	▲			▲	▲	▲	▲
BIG-IP v11.5.2	▲	▼	▲	▼	▼	▼	▼	▲	▲	▲	▲	▲	▲			▲	▲	▲	▲
BIG-IP v11.6.0	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲			▲	▲	▲	▲
BIG-IP v11.6.1	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲			▲	▲	▲	▲
BIG-IP v12.0.0	▲	▲	▲	▲	▲	▲		▲	▲	▲	▲	▲	▲	▼	▼	▲	▲	▲	▲

Max of String	DHE-DSS-AES128-SHA256	DHE-DSS-AES256-GCM-SHA384	DHE-DSS-AES256-SHA	DHE-DSS-AES256-SHA256	DHE-DSS-CAMELLIA128-SHA	DHE-DSS-CAMELLIA256-SHA	DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA256	DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA256	DHE-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA256-SHA	DHE-RSA-DES-CBC3-SHA	DHE-RSA-DES-CBC-SHA	DH-RSA-AES128-SHA	DH-RSA-AES256-SHA	DH-RSA-DES-CBC3-SHA	DH-RSA-DES-CBC-SHA
BIG-IP v10.2.1								▼			▼				▼	▼	▼	▼	▼	▼
BIG-IP v10.2.2								▼			▼				▼	▼				
BIG-IP v10.2.3								▼			▼				▼	▼				
BIG-IP v10.2.4								▼			▼				▼	▼				
BIG-IP v11.0.0								▼			▼				▼	▼				
BIG-IP v11.1.0								▼			▼				▼	▼				
BIG-IP v11.2.0								▼			▼				▼	▼				
BIG-IP v11.2.1								▲			▲				▲	▲				
BIG-IP v11.3.0								▲			▲				▲	▲				
BIG-IP v11.4.0								▲			▲				▲	▲				
BIG-IP v11.4.1								▲			▲				▲	▲				
BIG-IP v11.5.0	▲	▲	▲	▲			▲	▲		▲	▲				▲	▲				
BIG-IP v11.5.1	▲	▲	▲	▲			▲	▲		▲	▲				▲	▲				
BIG-IP v11.5.2	▲	▲	▲	▲			▲	▲	▲	▲	▲	▲			▲	▲				
BIG-IP v11.6.0	▲	▲	▲	▲			▲	▲		▲	▲				▲	▲				
BIG-IP v11.6.1	▲	▲	▲	▲			▲	▲		▲	▲				▲	▲				
BIG-IP v12.0.0	▲	▲	▲	▲	▼	▼	▲	▲	▲	▲	▲	▲	▼	▼	▲	▲				

Max of String	ECDH-ECDSA-AES128-GCM-SHA256	ECDH-ECDSA-AES128-SHA	ECDH-ECDSA-AES128-SHA256	ECDH-ECDSA-AES256-GCM-SHA384	ECDH-ECDSA-AES256-SHA	ECDH-ECDSA-AES256-SHA384	ECDH-ECDSA-DES-CBC3-SHA	ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE-ECDSA-AES128-SHA	ECDHE-ECDSA-AES128-SHA256	ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE-ECDSA-AES256-SHA	ECDHE-ECDSA-AES256-SHA384	ECDHE-ECDSA-DES-CBC3-SHA	ECDHE-RSA-AES128-CBC-SHA	ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-SHA256	ECDHE-RSA-AES256-CBC-SHA	ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-SHA384	ECDHE-RSA-DES-CBC3-SHA
BIG-IP v10.2.1																					
BIG-IP v10.2.2																					
BIG-IP v10.2.3																					
BIG-IP v10.2.4																					
BIG-IP v11.0.0																					
BIG-IP v11.1.0																					
BIG-IP v11.2.0																					
BIG-IP v11.2.1																					
BIG-IP v11.3.0																					
BIG-IP v11.4.0															▲			▲			▲
BIG-IP v11.4.1															▲			▲			▲
BIG-IP v11.5.0	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
BIG-IP v11.5.1	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
BIG-IP v11.5.2	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
BIG-IP v11.6.0	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
BIG-IP v11.6.1	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
BIG-IP v12.0.0	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲

Max of String	ECDH-RSA-AES128-GCM-SHA256	ECDH-RSA-AES128-SHA	ECDH-RSA-AES128-SHA256	ECDH-RSA-AES256-GCM-SHA384	ECDH-RSA-AES256-SHA	ECDH-RSA-AES256-SHA384	ECDH-RSA-DES-CBC3-SHA	EXP1024-DES-CBC-SHA	EXP1024-RC2-CBC-MD5	EXP1024-RC4-MD5	EXP1024-RC4-SHA	EXP-ADH-DES-CBC-SHA	EXP-ADH-RC4-MD5	EXP-DES-CBC-SHA	EXP-DH-RSA-DES-CBC-SHA	EXP-EDH-RSA-DES-CBC-SHA	EXP-RC2-CBC-MD5	EXP-RC4-MD5	RC4-MD5	RC4-SHA
BIG-IP v10.2.1								▲	▼	▲	▲	▼	▼	▲	▼	▼	▼	▲	▲	▲
BIG-IP v10.2.2								▲	▼	▲	▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v10.2.3								▲	▼	▲	▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v10.2.4								▲	▼	▲	▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.0.0								▲	▼	▲	▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.1.0								▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.2.0								▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.2.1								▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.3.0								▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.4.0								▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.4.1								▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.5.0	▲	▲	▲	▲	▲	▲	▲	▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.5.1	▲	▲	▲	▲	▲	▲	▲	▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.5.2	▲	▲	▲	▲	▲	▲	▲	▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.6.0	▲	▲	▲	▲	▲	▲	▲	▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v11.6.1	▲	▲	▲	▲	▲	▲	▲	▲			▲	▼	▼	▲		▼	▼	▲	▲	▲
BIG-IP v12.0.0	▲	▲	▲	▲	▲	▲	▲													▲

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113