Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Direct: 408 526 4000
FAX: 408 526 4100
www.cisco.com

July 21, 2014

To Whom It May Concern

Cisco completed its conformance review of Sourcefire 3D System software (Version: 5.2)("the Product") on July 21, 2014, and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

1. OpenSSL FIPS Object Module (FIPS 140-2 Cert. #1051)

Specifically, Cisco's review confirmed that:

The Product utilizes a FIPS 140-2 validated cryptographic module certificate #1051[1] (i.e., OpenSSL FIPS Object Module or FOM) providing Approved cryptographic functions. The algorithm implementations have been tested and validated in accordance to the validation suites set by the Cryptographic Algorithm Validation Program (CAVP). The following algorithms have been FIPS validated in accordance with the identified standards:

Table 21: FIPS 140-2 Algorithms

Algorithms	Standards	Certificate Numbers
Asymmetric Key Generation		
• Domain parameter generation	NIST Special Publication 800-56B NIST Special Publication 800-57	#1227
• Random number generation	See RBG below	
Encryption/Decryption		
• AES (128, 192, and 256 bits) in CBC mode	FIPS PUB 197 NIST SP 800-38A	#2575
Cryptographic Signature Services		

[1] Please see the Security Policy for more information:
http://www.openssl.org/docs/fips/SecurityPolicy-1.2.2.pdf

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Direct: 408 526 4000
FAX: 408 526 4100
www.cisco.com

• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS PUB 186-2	#1322
Cryptographic Hashing		
• SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 (digest sizes 160, 224, 256, 384 and 512 bits)	FIPS PUB 180-3	#2174
Keyed-hash Message Authentication		
• HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 (message digest sizes 160, 224, 256, 384, and 512 bits)	FIPS PUB 198-1 FIPS PUB 180-3	#1598
Random Bit Generation (RBG)		
• RBG with independent software-based noise source of 128 bits	FIPS PUB 140-2 Annex C: X9.31 Appendix 2.4 using AES	#1227

Cisco verified that the FOM was compiled as specified in the Security Policy and User Guide. Cisco also verified that the following service/protocol uses the cryptographic functions provided by the FOM: TLS, HTTPS, and SSH. Finally, Cisco verified that the Product invokes the FIPS self-tests of the FOM and will not enter operational mode until all of the self-test successfully pass.

The intention of this letter is to provide our assessment that the Product correctly integrates and uses validated cryptographic modules within the scope of the claims indicated above. Cisco offers no warranties or guarantees with respect to the above described conformance review. Furthermore, the Cryptographic Module Validation Program (CMVP) has not independently reviewed Cisco's analysis, testing or results.

Any questions regarding these statements may be directed to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

Thomas Ashoff

VP Engineering