CISCO

Cisco Systems, Inc.
7025 Kit Creek Road
P.O. Box 14987
Research Triangle Park
NC 27709
Phone: 919 392-2000
http://www.cisco.com

May 9, 2014

To Whom It May Concern

Cisco completed its conformance review of Cisco Email Security Appliance (ESA) (Version: 8.0.2)("the Product") on May 8, 2014, and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

1.   Cisco Common Crypto Module (C3M) (FIPS 140-2 Cert. #1643)

Specifically, Cisco's review confirmed that:

1.   The integrated cryptographic module (mentioned above) is initialized in a manner that is compliant with their individual security policy.
2.   All cryptographic algorithms used in TLSv1/HTTPs and SSHv2 for session establishment, as well as bulk data encryption, are offloaded to Cisco Common Crypto Module (C3M) version 0.9.8r.1.1
3.   All cryptographic algorithms used in SCP for secure copying and bulk data encryption are offloaded to Cisco Common Crypto Module (C3M) version 0.9.8r.1.1
4.   All cryptographic algorithms used in DomainKeys Identified Mail for digital signatures are offloaded to Cisco Common Crypto Module (C3M) version 0.9.8r.1.1
5.   The Product's services will not operate if the integrated FIPS validated module (mentioned above) is missing or altered.

Details of Cisco's review, which consisted of source code review and operational testing, can be provided upon request.

Moreover, the FIPS conformance claims made for Cisco Common Crypto Module (C3M), (FIPS 140-2 Cert. #1643), hold true for Cisco Email Security Appliance (ESA) (Version: 8.0.2) with no additions or removal of cryptographic services or cryptographic implementations.

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,

Ed Paradise
VP Engineering
Cisco TRIAD