DECEMBER 2014

Cisco Adaptive Security Appliance (ASA) version 9.1(2)

Product Description

The Cisco Adaptive Security Appliance (Cisco ASA) provides both IPsec VPN and firewall functionality and consists of the following components: ASA 5500 (5505, 5510, 5520, 5540, 5550, 5580-20-40), ASA 5500-X Series (5512-X, 5515-X, 5525-X, 5545-X, 5555-X), ASA 5585-X (5585-10, 5585-20, 5585-40, 5585-60), ASA Services Module (ASA-SM).

The Cisco ASA consists of both hardware and software solutions to provide application-aware stateful packet filtering firewalls. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the authorised administrator for firewalls.

The Cisco ASA can operate in a number of modes: as a single standalone device with a single-context, or with multiple-contexts within each single/pair; as a transparent firewall when deployed in a single-context, or with one or more contexts connected to two or many IP subnets when configured in router mode.

For management purposes, the Adaptive Security Device Manager (ASDM) is included. ASDM allows the ASA to be managed from a graphical user interface.

Evaluation Scope

The scope of the ASD Cryptographic Evaluation (ACE) included the following functionality:

- Authentication
- Data confidentiality
- Data integrity

Protection Profile Conformance – Summary

The product was found to comply with the Networked Device Protection Profile (NDPP) v1.1 and Traffic Filter Firewall Extended Package (TFFWEP) v1.0.

ASD Findings and Recommendations

ASD performed a cryptographic evaluation on the product in addition to the NDPP and TFFWEP conformance testing.

As the product has successfully completed an ACE, it can be used to downgrade the requirements of PROTECTED data in transit to those of UNCLASSIFIED, in accordance with the Australian Government Information Security Manual (ISM).

Recommendations given in this Consumer Guide take precedence over those in the ISM where there is a conflict.

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

ISM

The advice given in this document is in accordance with the Information Security Manual 2014. Australian government agencies are reminded to periodically check the latest release date of the ISM at www.asd.gov.au/infosec/ism/

Consumer Guide

This Consumer Guide was issued by ASD during December 2014.

(U) **LEGAL WARNING**: ALL DOCUMENTS ORIGINATING WITH OR RECEIVED FROM ASD ARE EXEMPT UNDER SECTION 7(2A) OF THE *FREEDOM OF INFORMATION (FOI) ACT 1982*. THIS EXEMPTION EXTENDS TO DOCUMENTS THAT CONTAIN SUMMARIES OF AN ASD DOCUMENT OR EXTRACTS FROM SUCH A DOCUMENT. ASD MUST BE CONSULTED PRIOR TO THE RELEASE OF ANY SUCH INFORMATION UNDER AN FOI REQUEST.