0122

CERTIFICATION REPORT No. CRP276

Cisco Catalyst 4500 Series switches (4503-E, 4506-E, 4507R+E, 4510R+E, 4500X and 4500X-F) running IOS-XE 3.5.2E

Issue 1.0

April 2014

CESG Certification Body
IA Service Management, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme ('the Scheme') and has met the specified Common Criteria (CC) [CC] requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this Certification Report.

Sponsor	Cisco Systems Inc	Developer	Cisco Systems Inc
Product(s), Version(s)	Cisco Catalyst 4500 Series switches (4503-E, 4506-E, 4507R+E, 4510R+E, 4500X and 4500X-F) running IOS-XE 3.5.2E		
Platform(s)	N/A		
Description	Each Catalyst 4500 Series switch is a network device (a switching/routing platform) used to build IP networks by interconnecting multiple smaller networks or network segments		
CC Version	Version 3.1 Release 3		
CC Part 2	Extended	CC Part 3	Conformant
PP Conformance	Strictly conformant with Network Devices PP v1.0		
EAL or [c]PP	Network Devices PP v1.0		
CLEF	CGI (ex-Logica) CLEF (LFL)		
CC Certificate	P276	Date Certified	30 April 2014

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE) in meeting its Security Target (ST) [ST], which prospective consumers are advised to read. To ensure that the ST gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline. Both parts of the evaluation were performed in accordance with Network Devices PP v1.0 [PP], CC Parts 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issuing of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this Certification Report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

SENIOR OFFICIALS GROUP – INFORMATION SYSTEMS SECURITY (SOGIS) MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (MRA)

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to the above Agreement [MRA] and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

CCRA logo **CC logo** **SOGIS MRA logo**

[1] All judgements contained in this Certification Report, are covered by the CCRA [CCRA] and the SOGIS MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of the product identified below (and on Page 2 'Certification Statement'). It is addressed to the Sponsor of this evaluation, Cisco Systems Inc, and it is also intended to assist prospective consumers when judging the suitability of the product's IT security features to meet their particular requirements.

2. Prospective consumers of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements that the product was evaluated against.

Evaluated Product and TOE Scope

3. The following Cisco Catalyst 4500 Series switch models completed evaluation against the Network Devices Protection Profile v1.0 [PP] on 14 February 2014:

- Cisco Catalyst 4500 Series switches (4503-E, 4506-E, 4507R+E, 4510R+E, 4500X and 4500X-F) running IOS-XE 3.5.2E.

4. Hereinafter, the above models are collectively referred to as the 'Cisco Catalyst 4500 Series switches' or 'the set of TOEs'. Further model identification details - e.g. chassis and card ids - are given in Chapter III 'Evaluated Configuration' of this report.

5. A statement in this report about the 'TOE' (Target of Evaluation) or 'the product' applies to each of the above models (unless stated otherwise). The Developer of the TOE is Cisco Systems Inc.

6. The TOE is a network device (a switching/routing platform) used to build IP networks by interconnecting multiple smaller networks or network segments. Further details are given in Chapter IV 'Product Architecture' of this report.

7. Details of the TOE Scope, and the TOE's assumed environment and evaluated configuration, are given in Chapter III 'Evaluated Configuration' of this report. Configuration requirements are specified in Sections 1.3.3, 1.5 and 1.8 of [ST]. Note, in particular, that the evaluated configuration requires that the TOE be connected to the following generic non-TOE components:

- An authentication server (RADIUS or TACACS+);
- A management workstation with SSHv2 Client;
- A syslog server.

8. The evaluated configuration also requires that traffic passing between the TOE and the authentication server and the syslog server must be protected by an IPsec IKEv1 connection.

Protection Profile Conformance

9. The Security Target [ST] is certified as achieving *strict* conformance to the following protection profile:

- Security Requirements for Network Devices, Information Assurance Directorate (IAD), Version 1.0, 10 December 2010 [PP].

Security Target

10. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats which these Objectives counter, the Organisational Security Policies (OSPs) which these Objectives meet and the Security Functional Requirements (SFRs) that refine these Objectives. Most of the SFRs are taken from CC Part 2 [CC2], and all of them are taken from [PP]; this facilitates comparison with other evaluated products.

11. The TOE security policies are detailed in [ST]. The OSPs that must be met are specified in Section 3.6 of [ST]. (In fact, there is just one OSP, which is that the TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.)

12. The environmental assumptions related to the operating environment are outlined in Chapter III ('Environmental Requirements' section) of this report.

Cryptographic Mechanisms

13. The TOE contains a number of cryptographic mechanisms that are used to implement the SSHv2 and IPsec IKEv1 cryptographic protocols that are supported by the TOE. These mechanisms are publicly known and as such it is the policy of CESG, as the UK National Technical Authority for cryptographic mechanisms, not to comment on their appropriateness or strength. However, the Evaluators confirmed that the implementation of these mechanisms had successfully achieved Federal Information Processing Standard (FIPS) 140-2 certifications (Certificate No. 1940 and 2116).

Evaluation Conduct

14. The evaluation was primarily performed against [PP], using [CC] and the methods and techniques defined in [CEM] wherever possible. In the event of a conflict between [PP] and [CC] or [CEM], [PP] was given precedence, and details of the conflict were formally communicated to the CESG Certification Body (CB) by recording them in an Observation Report (OR) level 4.

15. The CESG Certification Body monitored the evaluation, which was performed by the CGI (ex-Logica) Commercial Evaluation Facility (CLEF), and witnessed a sample of Evaluator tests. The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in February 2014, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

16. The TOE should be used in accordance with the environmental assumptions specified in the Security Target [ST]. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

17. The TOE should be used in accordance with its supporting guidance documentation (identified in Chapter II 'TOE Security Guidance' of this report).

Conclusions

18. The conclusions of the CESG Certification Body are summarised on Page 2 'Certification Statement' of this report.

Recommendations

19. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure delivery, receipt, installation, configuration and operation of the TOE.

20. In its evaluated configuration the TOE needs to be connected to other components (identified generically in Paragraph 7 of this report). No requirements are placed on these components in [ST]; however, System integrators and risk owners using the TOE in its evaluated configuration should make suitable arrangements to satisfy themselves that they have appropriate confidence that the specific non-TOE components that are deployed function correctly and are used in an adequately secure manner.

21. The Evaluators' comments and recommendations are as follows:

- The Developer should ensure that the guidance document [AG] (or a URL link to it) is shipped with the TOE to the Developer's customers (i.e. to the TOE consumers);

- When planning to deploy the TOE in its evaluated configuration, consumers should pay particular attention to the IPsec requirement stated in Paragraph 8 of this report. Note that it may not be possible to establish an IPsec connection from the TOE that terminates on the platform that hosts the authentication and/or syslog server; this depends on the chosen hosting platform(s). If termination is not possible, then an additional component (a suitable routing device) must be used to terminate the IPsec connection from the TOE, with a physically secure connection between it (the additional component) and the server(s)' hosting platform(s). This point is elaborated in Section 3.3.4.7 of [AG];

- Consumers should also note that readers of [AG] are assumed to be fully trained in the use of IOS-XE software (see Paragraph 33 of this report). A person who is not so trained should not assume that - armed solely with [AG] and access to the thousands of pages of material referenced therein - it is a trivial task for him or her to configure the TOE to meet the requirements of [ST].

Disclaimers

22. This Certification Report and associated Certificate applies only to the specific version of the product in its evaluated configuration (i.e. the TOE). This configuration is specified in Chapter III 'Evaluated Configuration' of this report. The ETR on which this Certification Report is based relates only to the specific items tested.

23. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered after the Evaluators' penetration tests were completed. This report reflects the CESG Certification Body's view on that date (see Paragraph 62 of this report).

24. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the date of the penetration tests (as detailed in Chapter V 'TOE Testing') and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

25. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE but should only be applied in accordance with a consumer's risk management policy. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

26. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

27. Note that the opinions and interpretations stated in this report in Chapter I ('Recommendations' section) and Chapter II 'TOE Security Guidance' are based on the experience of the CESG Certification Body in performing similar work under the Scheme.

II. TOE SECURITY GUIDANCE

Introduction

28. The following sections provide guidance that is of particular relevance to consumers of the TOE.

Delivery and Installation

29. On receipt of the TOE (hardware and software), the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised during delivery. Specific advice on delivery and installation is provided in Section 2 of [AG] (see 'Guidance Documents' section below). This includes instructions on how to verify that the software (the IOS-XE 3.5.2E image file, which implements all the evaluated security features of the TOE) was not tampered with (by using an MD5 utility to compute an MD5 hash for the image file and comparing this with the value listed in Table 2 of [AG]).

30. In addition, Section 4.2 of [AG] includes two script files and instructions for installing them into the TOE. **If this installation is not done then the TOE is not in its evaluated configuration**.

Guidance Documents

31. The Administration Guide [AG] documentation is as follows:

- Cisco Catalyst 4500 Series Switches (4503-E, 4506-E, 4507R+E, 4510R+E, 4500X and 4500X-F) Running IOS-XE 3.5.2E Common Criteria Operational User Guidance and Preparative Procedures, Cisco Systems Inc, EDCS–1228243, Version 1.0, 11 February 2014.

32. This document includes specific configuration advice, plus over twenty references to other relevant Cisco documents, such as command reference manuals, that are available from Cisco's web site. There is no separate User Guide, because all users of the TOE are administrators (to a greater or lesser extent - different users can be assigned different privilege levels).

33. The consumer should be aware that Section 1.1 of [AG] states (bold face added in this report for emphasis):

- 'This document is written for administrators configuring the TOE, specifically the IOS XE software. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that **you are trained to use IOS XE software and the various operating systems on which you are running your network**'.

III. EVALUATED CONFIGURATION

TOE Identification

34. The TOE is identified as Cisco Catalyst 4500 Series switches (4503-E, 4506-E, 4507R+E, 4510R+E, 4500X and 4500X-F) running IOS-XE 3.5.2E.

35. Each of the first four of these switch types (4503-E thru 4510R+E) is actually a combination of the following components:

- One switch chassis (WS-C4503-E, WS-C4506-E, WS-C4507R+E or WS-C4510R+E);
- One or two supervisor cards installed in the chassis; if one card then it may be a WS-X45-SUP7-E card or a WS-X45-Sup7L-E card; if two cards, then they may be two WS-X45-SUP7-E cards or two WS-X45-Sup7L-E cards or a WS-X45-SUP7-E card plus a WS-X45-Sup7L-E card. Each installed card runs an instance of the IOS-XE 3.5.2E operating system software;
- One or more of each of the following five types of line card installed in the chassis: WS-X4748-RJ45V+E; WS-X4712-SFP+E; WS-X4640-CSFP-E; WS-X4748-UPOE+E; WS-X4748-RJ45-E. There must be at least one line card installed in a chassis, and the total number of line cards installed in a chassis is limited by the number of line card slots in that chassis. (The installed line cards need not be all of the same type.)

36. The other two switch types (4500X and 4500X-F) are actually a set of seven switches identified as follows: WS-C4500X-32SFP+; WS-C4500X-F-32SFP+; WS-C4500X-16SFP+; WS-C4500X-F-16SFP+; WS-C4500X-24X-ES; 4500X-24X-IPB; WS-C4500X-40X-ES.

37. Each of these seven switches is a self-contained unit running the IOS-XE 3.5.2E operating system software.

38. A ‘TOE instance’ is defined as being any meaningful (i.e. operationally viable) subset of the above collection of hardware switches/components (plus the operating system). Hence, for example, a chassis with a line card but no supervisor card installed in it is not a TOE instance.

TOE Documentation

39. The relevant guidance documents for the evaluated configuration are identified in Chapter II (‘Guidance Documents’ section) of this report.

TOE Scope

40. The TOE Scope is defined in Sections 1.6 and 1.7 of [ST]. Functionality that is outside the TOE Scope is defined in Section 1.8 of [ST], namely:

- HTTP/HTTPS, SNMP and telnet servers;
- IEEE 802.11 wireless capability and VPN Remote Access;
- Smart Install and TrustSec.

41. The above functionality of the TOE must be disabled in the TOE's evaluated configuration.

42. Other TOE functionality need not be disabled, but it may be outside the scope of the TOE's security functionality (if it does not directly implement an SFR specified in [ST]). A particular example of this is the functionality supporting information flow policies (see Section 1.2 of [AG]). Other examples include configuring two switch chassis together to provide a Virtual Switching System (VSS) that supports High Availability (HA); and employing two supervisor cards in one chassis to provide a supervisor failover capability.

TOE Configuration

43. The evaluated configuration of the TOE is defined in Sections 1.3.3, 1.5 and 1.8 of [ST], and specific configuration advice is provided throughout [AG].

44. The diagram overleaf (which is Figure 1 in [ST]) depicts the TOE in its evaluated configuration (excluding the 'NTP Server', which is optional).

Environmental Requirements

45. The environmental assumptions for the TOE are stated in Section 3.4 of [ST]. They are mainly concerned with physical and personnel security measures.

46. The environmental IT configuration (excluding the 'NTP Server', which is optional) is depicted in the diagram overleaf, in which:

- The Catalyst 4K Switch is a TOE instance;
- The NTP Server is optional and should be ignored for the purposes of this Certification Report;
- The Administration, Authorisation and Accounting (AAA) Server is a RADIUS or TACACS+ server;
- The Peer is a neighbour network device on the TOE's untrusted or 'external' network, in contrast to the Management (Mgt) Workstation and Servers, which are on the TOE's (relatively) trusted or 'internal' network;

- A local administration console - not shown in the diagram - may be attached directly to the TOE's console port.

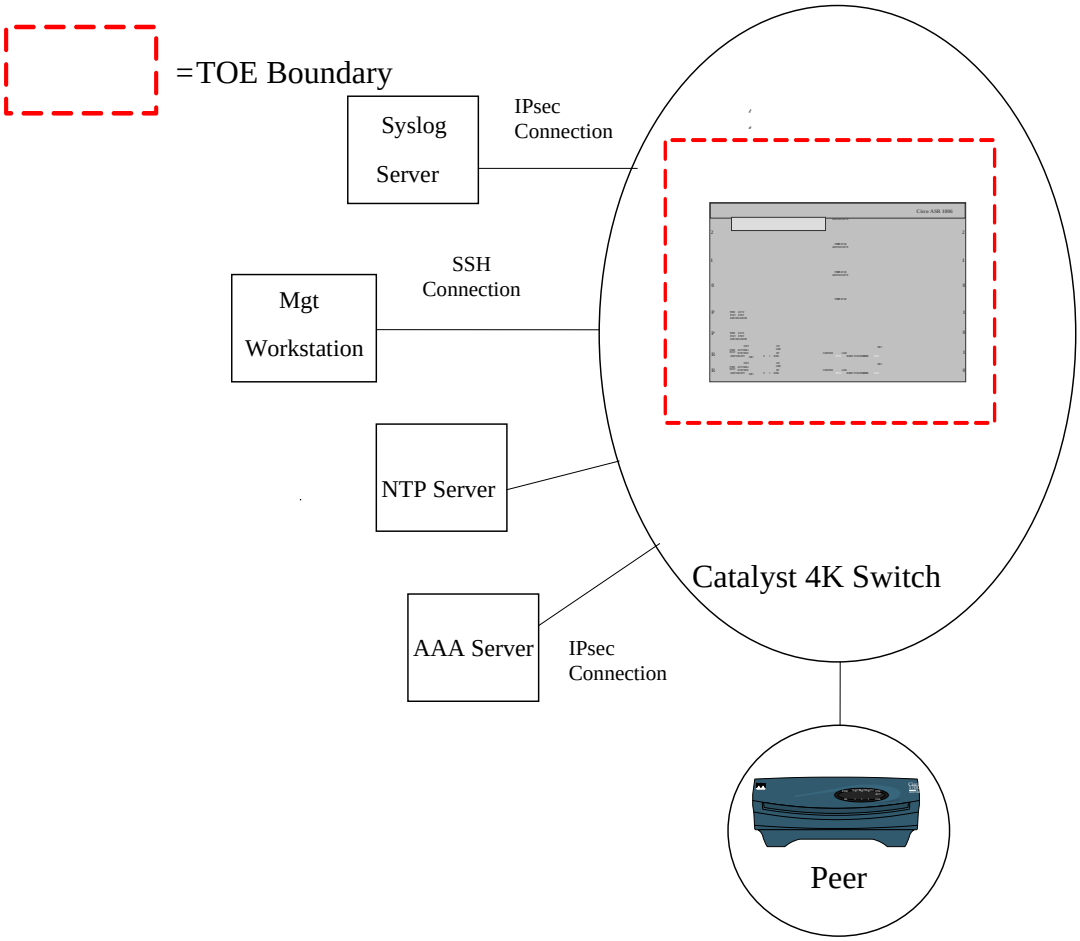

Figure 1: Environmental IT Configuration

Test Configurations

47. Details of the Developer's test configuration are not provided (because they were not required by the evaluation).

48. The Evaluators used the following equipment for their testing:

- Two instances of the TOE (referred to as the 4507 and the 4500X). The 4507 TOE instance consisted of a WS-C4507R+E chassis containing a WS-X45-SUP7-E supervisor card and a WS-X4748-RJ45V+E line card; the 4500X TOE instance was a WS-C4500X-40X-ES switch;

- Both TOE instances were running IOS-XE 3.5.0E (bootflash:cat4500e-universalk9.SPA.03.05.00.E.152-1.E.bin), configured as specified in [AG]; in particular, two additional script files were installed in both TOE instances (see Section 4.2 of [AG]);

- A Cisco 800 series router (used to terminate IPsec connections from the TOE instances, see Paragraph 21 of this report);

- Three laptops, each running Windows 7 Enterprise, and collectively hosting the following software: Wireshark v1.10.0 from wireshark.org; PuTTY v0.62 from putty.org; Syslog server v1.2.3 from sourceforge.net; RADIUS server v2.2.0 from sourceforge.net; FTP server v0.9.41 from filezilla-project.org.

49. This equipment was connected together into a test network as per the above diagram (excluding the optional NTP server).

50. Clearly, the Evaluators' test configuration does not cover all possible TOE instances (as defined in Paragraph 38 of this report). However, the Evaluators' test results may be extrapolated to the whole set of TOEs because the IOS software implements all the SFRs specified in [ST] regardless of the particular TOE hardware on which it runs. The test results may also be extrapolated to IOS-XE 3.5.2E because:

- IOS-XE 3.5.2E was released on 28 March 2014 to fix a Denial of Service vulnerability in the IOS-XE 3.5.0E implementation of IKE v2;

- The TOE is not in its evaluated configuration if it is configured to use IKE v2 (rather than IKE v1);

- IOS-XE 3.5.2E is the subject of FIPS 140-2 Certificate No. 2116.

IV. PRODUCT ARCHITECTURE

Introduction

51. This Chapter gives an overview of the TOE's main architectural features. Other details of the scope of the evaluation are given in Chapter III 'Evaluated Configuration' of this report.

Product Description and Architecture

52. An architectural description of the TOE is given in Sections 1.3 and 1.4 of [ST]; some key points may be summarised as follows.

53. The TOE is a network device (a switching/routing platform) used to build IP networks by interconnecting multiple smaller networks or network segments. Considering any TOE instance:

- The supervisor and line cards are fitted into slots in the chassis (or are, in effect, already installed inside the 4500X series outer cases);
- Traffic (Layer 2 frames or Layer 3 packets) from the external network - see Chapter III ('Environmental Requirements' section) of this report - is received on a line card port and passed to a supervisor card for processing (which, in essence, consists of consulting the relevant routing table to determine what to do with the frame or packet), then either dropped or passed to an appropriate line card port for onward transmission;
- Traffic from the internal network - see Chapter III ('Environmental Requirements' section) of this report - is handled in a similar manner (except that it may be received on or transmitted from a supervisor card port directly);
- The switch is administered via a command line interface (CLI), which can be accessed either locally (by plugging a console into a supervisor card port) or remotely (via the internal network); administration includes configuring the routing tables. (However, the configuration and operation of routing tables is not addressed by [ST] or [PP], and hence is outside the scope of the evaluation);
- The hardware/firmware of the chassis and cards does not affect the TSF, which is implemented entirely by the IOS software running on the supervisor card(s). (Note that this software must be configured into the 'evaluated configuration' - as specified in [AG] and outlined in Chapter III 'Evaluated Configuration' of this report - for the TOE to satisfy the requirements of [ST].)

TOE Design Subsystems

54. Details of the high-level TOE subsystems, and their security features/functionality, are not provided (because they are not required by [ST] or [PP]). However, Section 1.7 of [ST] describes the security features of the TOE under the following sub-headings: Security audit; Cryptographic support; User data protection; Identification and authentication; Secure management; Protection of the TSF; Resource utilisation; TOE access; Trusted path/channel.

TOE Dependencies

55. The TOE itself is self-contained, i.e. it has no dependencies on any other hardware or software. However, in order to function in its evaluated configuration, the TOE needs to be connected to the generic non-TOE components listed in Paragraph 7 of this report.

TOE Security Functionality Interfaces

56. The external TOE Security Functionality Interface (TSFI) consists of the following interfaces (see Sections 1.6.1 - 1.6.3 of [ST]):

- USB console port - this allows a management console to be connected to the TOE as a USB device;
- Network ports - these are Ethernet interfaces allowing connections to the internal and external networks. Interface speeds vary by TOE instance, e.g some instances have Small Form-Factor Pluggable Plus (SFP+) interfaces that support both 10 gigabit and 1 gigabit speeds; others have conventional 10/100/1000 megabit Ethernet interfaces. (Further details are given in Section 1.6 of [ST]);
- Serial port - this allows a management console to be connected to the TOE via RS-232 signalling over an RJ45 interface.

57. Some TOE instances also include a compact flash slot, to which a compact flash drive may be fitted to provide extra storage capacity. However, this physical interface is considered to be internal to the TOE, i.e. it is not part of the external TSFI (see Section 1.6.4 of [ST]).

V. TOE TESTING

Developer Testing

58. Details of the Developer's testing of the TOE are not provided (because they are not required by [ST] or [PP]).

Evaluator Testing

59. The Evaluators devised and performed a total of nineteen independent security functional tests. No anomalies were found.

60. The Evaluators also devised and performed a total of six penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

61. Functional and penetration tests were performed by the Evaluators using the test network summarised in Chapter III ('Test Configurations' section) of this report.

62. The Evaluators completed their penetration tests on 31 January 2014.

Vulnerability Analysis

63. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

Platform Issues

64. The Evaluators did not identify any platform issues that should be considered by consumers, apart from the potential difficulty of terminating an IPsec connection from the TOE on the platform that hosts the authentication and/or syslog server (see Paragraph 21 of this report).

VI. REFERENCES

[AG] Cisco Catalyst 4500 Series Switches (4503-E, 4506-E, 4507R+E, 4510R+E, 4500X and 4500X-F) Running IOS-XE 3.5.2E Common Criteria Operational User Guidance and Preparative Procedures,
Cisco Systems Inc,
EDCS–1228243, Version 1.0, 11 February 2014.

[CC] Common Criteria for Information Technology Security Evaluation (comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2009-07-001, Version 3.1 R3, July 2009.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Components,
Common Criteria Maintenance Board,
CCMB-2009-07-002, Version 3.1 R3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Components,
Common Criteria Maintenance Board,
CCMB-2009-07-003, Version 3.1 R3, July 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
May 2000.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2009-07-004, Version 3.1 R3, July 2009.

[ETR] Evaluation Technical Report,
CGI (ex-Logica) CLEF,
LFL/T276/ETR EC232534.9.1, Issue 1.0, February 2014
supplemented by
CESG Certification Body Review Form,
CB/140218/LFL/T276, 28 April 2014.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee,
Senior Officials Group – Information Systems Security (SOGIS),
Version 3.0, 8 January 2010 (effective April 2010).

[PP] Security Requirements for Network Devices,
Information Assurance Directorate (IAD),
Version 1.0, 10 December 2010.

[ST] Cisco Catalyst 4500 Series Switches (4503-E, 4506-E, 4507R+E, 4510R+E, 4500X and 4500X-F) Running IOS-XE 3.5.2E Security Target,
Cisco Systems Inc,
EDCS-1228241, Revision 1.0, 11 March 2014.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.8, August 2013.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.5, August 2013.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.5, August 2013.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 3.1, August 2013.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. URL, IPsec, SSH, IKE); standard CC abbreviations (e.g. TOE, TSF) in CC Part 1 [CC1]; and UK Scheme abbreviations and acronyms (e.g. CLEF) in [UKSP00].

N/A	Not Applicable
NDPP	Network Devices Protection Profile
RADIUS	Remote Authentication Dial In User Service
TACACS+	Terminal Access Controller Access Control System (enhanced)

VIII. CERTIFICATE

The final two pages of this document contain the Certificate (front and back) for the TOE.

CESG CERTIFICATION BODY

CERTIFICATE No.
P276

This Certificate confirms that

Cisco Catalyst 4500 Series switches (4503-E, 4506-E, 4507R+E, 4510R+E, 4500X and 4500X-F) running IOS-XE 3.5.2E

has been evaluated under the terms of the

UK IT Security Evaluation and Certification Scheme

and complies with the requirements for

NDPP Version 1.0

(Security Requirements for Network Devices, Version 1.0, 10 December 2010)

The scope of the evaluated functionality was as claimed by the Security Target and as confirmed by the associated Certification Report **CRP276**.

Certification is not a guarantee of freedom from security vulnerabilities. This certificate reflects the CESG Certification Body's view at the time of certification. It is the responsibility of users (existing and prospective) to check whether any security vulnerabilities have been discovered since the date of the Evaluators' final penetration tests.

AUTHORISATION
Director for Information Assurance

DATE
30 April 2014

0122

0122

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to ***EN 45011:1998 (ISO/IEC Guide 65:1996)*** to provide product conformity certification as follows:

Category: Type Testing Product Certification of IT Products and Systems.

Standards:
- Common Criteria for Information Technology Security Evaluation (CC) EAL1 - EAL7; and
- Information Technology Security Evaluation Criteria (ITSEC) E1 - E6.

Details are provided on the UKAS website (www.ukas.org).

Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA), May 2000

The CESG Certification Body is a Participant to the above Arrangement. The current Participants to the above Arrangement are detailed on the Common Criteria Portal (www.commoncriteriaportal.org). The mark (left) confirms that this Common Criteria certificate has been authorised by a Participant to the above Arrangement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Arrangement. Upon receipt of this Common Criteria certificate, the vendor(s) may use the mark in conjunction with advertising, marketing and sales of the IT product for which this certificate is issued.

All judgements contained in this certificate, and in the associated Certification Report, are covered by the Arrangement.

Senior Officials Group – Information Systems Security (SOGIS)
Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA), Version 3.0

The CESG Certification Body is a Participant to the above Agreement. The current Participants to the above Agreement are detailed on the SOGIS Portal (www.sogisportal.eu). The mark (left) confirms that this conformant certificate has been authorised by a Participant to the above Agreement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Agreement. The judgments contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the mark does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

All judgements contained in this certificate, and in the associated Certification Report, are covered by the Agreement.

The IT product identified in this certificate has been evaluated by the CGI Commercial Evaluation Facility (an accredited and approved Evaluation Facility of the UK) using the ***Common Methodology for Information Technology Security Evaluation***, ***Version 3.1*** for conformance to the ***Common Criteria for Information Technology Security Evaluation, Version 3.1***. This certificate applies only to the specific version and release of the IT product listed in this certificate in its evaluated configuration and in conjunction with the complete, associated Certification Report. The evaluation has been conducted in accordance with the provisions of the UK IT Security Evaluation and Certification Scheme, and the conclusions of the Evaluation Facility in the Evaluation Technical Report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by CESG or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CESG or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

In conformance with the requirements of ***EN 45011:1998 (ISO/IEC Guide 65:1996)***, the ***CCRA*** and the ***SOGIS MRA***, the CESG Certification Body's website (www.cesg.gov.uk) provides additional information, as follows:

- type of product (i.e. product category); and
- details of product manufacturer (i.e. as appropriate: vendor/developer name, postal address, website, point of contact, telephone number, fax number, email address).