

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

For

X-ES Xpedite5205 Embedded Services Router

Report Number: CCEVS-VR-VID10576-2014
Dated: November 17, 2014
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Bradford O'Neill

Jean Petty

The MITRE Corporation

Jerome Myers

The Aerospace Corporation

Common Criteria Testing Laboratory

Kevin Micciche

Kevin Steiner

Anthony Apted

Gregory Beaver

Leidos (formerly SAIC, Inc.)
Columbia, MD

Table of Contents

1	EXECUTIVE SUMMARY	1
2	IDENTIFICATION	3
3	ARCHITECTURAL INFORMATION	3
3.1	PHYSICAL BOUNDARIES	5
3.2	CLARIFICATION OF SCOPE.....	5
4	SECURITY POLICY	6
4.1	SECURITY AUDIT	6
4.2	CRYPTOGRAPHIC SUPPORT	7
4.3	FULL RESIDUAL INFORMATION PROTECTION	7
4.4	IDENTIFICATION AND AUTHENTICATION.....	7
4.5	SECURITY MANAGEMENT	7
4.6	PACKET FILTERING.....	8
4.7	PROTECTION OF THE TSF	8
4.8	TOE ACCESS	8
4.9	TRUSTED PATH/CHANNELS	8
5	ASSUMPTIONS, THREATS, AND OSPS	9
5.1	ASSUMPTIONS	9
5.2	THREATS	9
5.3	ORGANIZATIONAL SECURITY POLICIES.....	10
6	DOCUMENTATION	10
7	PRODUCT TESTING.....	11
7.1	EVALUATED CONFIGURATION	11
7.1	INDEPENDENT TESTING.....	11
7.2	RESULTS OF THE EVALUATION.....	12
8	VALIDATOR COMMENTS/RECOMMENDATIONS	12
9	ANNEXES	13
10	SECURITY TARGET	13
11	ACRONYM LIST	13
12	BIBLIOGRAPHY.....	14

List of Tables

TABLE 1: ROUTER MODEL IN THE EVALUATED CONFIGURATION	1
TABLE 2: EVALUATION DETAILS.....	2
TABLE 3: ST AND TOE IDENTIFICATION.....	3
TABLE 4: DOCUMENTATION	10

List of Figures

FIGURE 1: TOE DEPLOYMENT EXAMPLE	5
--	---


1 Executive Summary

The evaluation of the X-ES XPedite5205 Cisco Embedded Services Router (ESR) running IOS 15.2(4)GC (herein after referred to as the XPedite5205) was performed by Leidos, in the United States and was completed in November 2014. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org). The criteria against which the XPedite5205 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 4. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation versions 3.1, revision 4.

Leidos Common Criteria Testing Laboratory determined that the product satisfies the Assurance Activities as defined within the Common Criteria (CC), the NDPPv1.1 with Errata #2 and VPNEPv1.1. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the X-ES Xpedite5205 Embedded Services Router Security Target, Version 1.0, October 13, 2014.

This Validation Report applies only to the specific version of the TOE as evaluated. The TOE is a hardware and software solution that makes up the router models as follows: ES XPedite5205 Embedded Services Router. The X-ES XPedite5205 is a rebranded Cisco ESR 5930. The network, on which they reside, is considered part of the environment. The software is comprised of the Universal Cisco IOS software image Release IOS 15.2(4) GC.

Table 1: Router Model in the Evaluated Configuration

Hardware	Picture	Interoperability	Size	Power	Interfaces
X-ES XPedite5205 (Standard Air-Cooled)		N/A	149 mm x 74 mm, 10 mm	Power will vary based on configuration and usage. Please consult factory.	(1) Serial Console Port (1) Auxiliary Port (4) 10/100/1000 Port LED signals
X-ES XPedite5205 (Rugged Air-Cooled)		N/A	149 mm x 74 mm, 10 mm	Power will vary based on configuration and usage. Please consult factory.	(1) Serial Console Port (1) Auxiliary Port (4) 10/100/1000 Port LED signals
X-ES XPedite5205 (Conduction-Cooled)		N/A	149 mm x 74 mm, 10 mm	Power will vary based on configuration and usage. Please consult factory.	(1) Serial Console Port (1) Auxiliary Port (4) 10/100/1000 Port LED signals

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and verdicts of the ETR. The validation team found that the evaluation showed that the product satisfies all of the security functional and assurance requirements stated in the Security Target (ST). The evaluation also showed that the product met all the security requirements and Assurance Activities contain in the Protection Profiles. Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced. This Validation Report is not an endorsement of the X-ES Xpedite5205 Embedded Services Router by any agency of the US Government and no warranty of the product is either expressed or implied.

The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Leidos evaluation team.

Table 2: Evaluation Details

Item	Identifier
Evaluated Product	X-ES Xpedite5205 Embedded Services Router
Sponsor & Developer	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	November 2014
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	U.S. Government Security Requirements for Network Devices (NDPP) version 1.1, 8 June 2012 Security Requirements for Network Devices Errata #2, January 2014 VPN Extended Package (VPNEP), Version 1.1, 12 April 2013
Evaluation Class	NDPP Errata #2 and VPNEP Assurance Requirements
Disclaimer	The information contained in this Validation Report is not an endorsement of the X-ES Xpedite5205 Embedded Services Router by any agency of the U.S. Government and no warranty of X-ES Xpedite5205 Embedded Services Router) is either expressed or implied.

Evaluation Personnel	Kevin Micciche Greg Beaver Kevin Steiner Dragua Zenelaj
Validation Personnel	Jean Petty Jerome Myers Bradford O'Neill

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM). The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

The following table serves to identify the evaluated Security Target and TOE.

Table 3: ST and TOE identification

Name	Description
ST Title	X-ES Xpedite5205 Embedded Services Router
ST Version	1.0
Publication Date	October 13, 2014
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	X-ES Xpedite5205 Embedded Services Router
TOE Hardware Models	X-ES XPedite5205 (Standard Air-Cooled) X-ES XPedite5205 (Rugged Air-Cooled) X-ES XPedite5205 (Conduction-Cooled)
TOE Software Version	Internetwork Operating System IOS 15.2(4)GC
Keywords	Router, Data Protection, Authentication, Firewall

3 Architectural Information

The Cisco X-ES Xpedite5205 Embedded Services Router is a router platform used to construct IP networks by interconnecting multiple smaller networks or network segments. The TOE provides connectivity and security services onto a single, secure device. The flexible, compact form factor of these routers, complemented by Cisco IOS® Software, provides highly secure data, voice, and video communications to stationary and mobile network nodes across wired links.

In support of the routing capabilities, the ESR provides IPsec connection capabilities for VPN enabled clients connecting through the ESR.

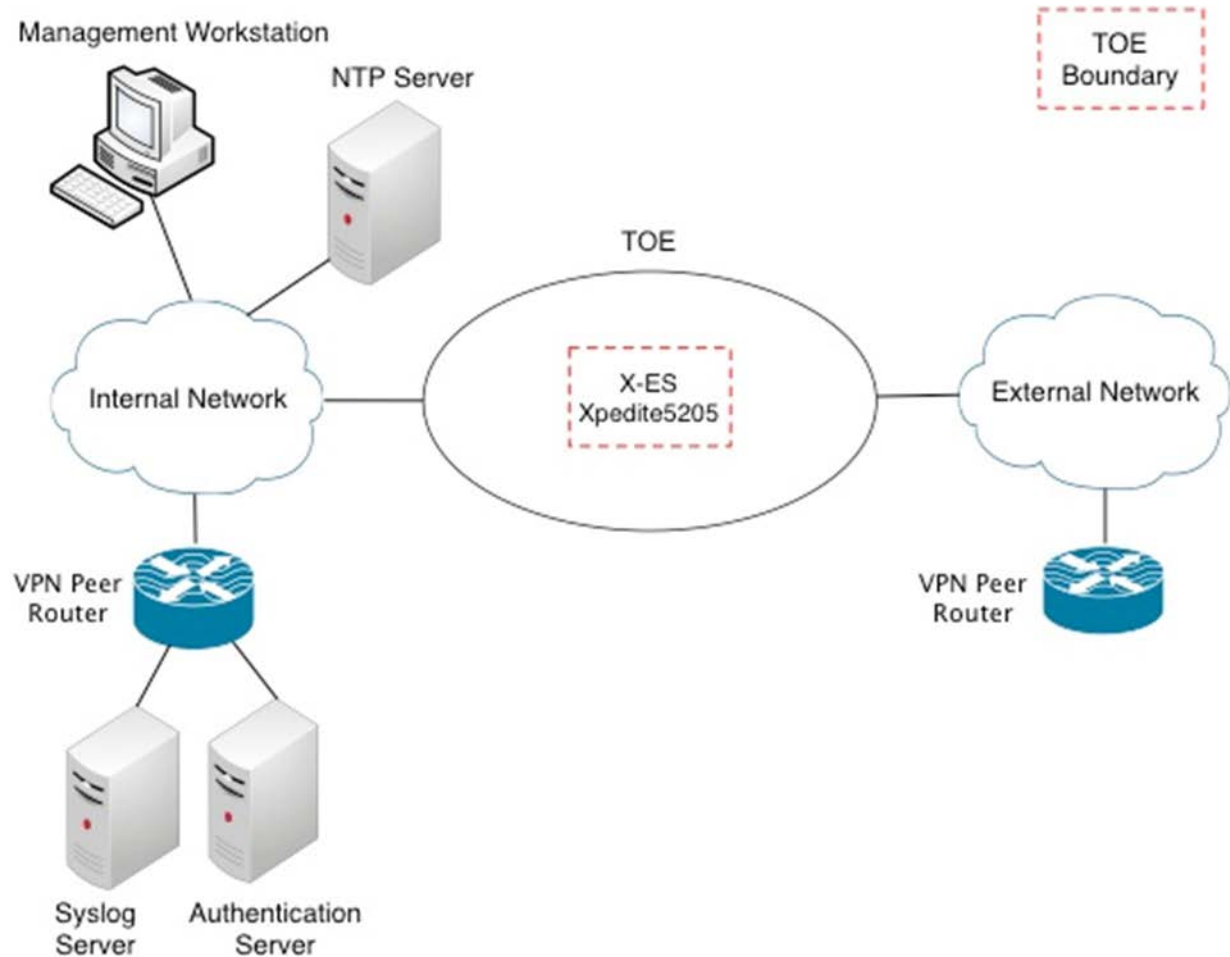
The ESR is a PCI-104 router module solution for protecting the network. The ESR provides routing, firewall, and VPN Gateway capabilities. The ESR controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the Authorized Administrator for firewalls. This header information includes source and destination host (IP) addresses, source and destination port numbers, and the transport service application protocol (TSAP) held within the data field of the IP packet. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The packet will be denied if the security policy is violated.

In addition to IP header information, the TOE mediates information flows on the basis of other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface. For connection-oriented transport services, the firewall either permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection.

The ESR can also establish trusted paths of peer-to-peer VPN tunnels. In addition, the ESR can act as a VPN Gateway by establishing secure VPN tunnels with IPsec VPN clients. Remote VPN clients are able to securely connect into the ESR over an encrypted session in order to connect to an authorized internal private network.

The following figure provides a visual depiction of an example TOE deployment.

Figure 1: TOE Deployment Example



3.1 Physical Boundaries

The TOE is a hardware and software solution that makes up the router models as follows: X-ES XPedite5205. The network, on which they reside, is considered part of the environment.

3.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.

3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
5. The following functionality is excluded from the evaluation: Non-FIPS 140-2 mode of operation on the TOE. The rationale for the exclusion is that Non-FIPS 140-2 mode of operation allows cryptographic operations that are not FIPS-approved. These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the Protection Profile for Network Devices and Network Device Protection Profile Extended Package VPN Gateway.
6. The TOE, when configured in its evaluated configuration, supports (in some cases optionally) the following hardware, software, and firmware in its operational environment:
 - a. RADIUS or TACACS+ AAA Server (optional)—can be used to provide external authentication services to the TOE
 - b. Management workstation with SSHv2 client—used by a TOE administrator to connect to the TOE for the purpose of remote administration
 - c. Local console—directly connected to the TOE via the Serial Console Port and used by the TOE administrator for the purpose of local administration
 - d. Certification Authority (optional)—can be used to provide the TOE with a valid certificate during certificate enrollment
 - e. Audit (syslog) server—an external audit server to which the TOE sends audit records (in the form of syslog messages)
 - f. Remote VPN endpoint—this includes any VPN peer or client with which the TOE participates in VPN communications. Remote VPN Endpoints may be any device or software client that supports IPsec or SSL (TLS) VPN communications. Both VPN clients and VPN gateways are considered to be Remote VPN Endpoints by the TOE
 - g. NTP server (optional)—the TOE supports communications with an NTP server in order to synchronize the date and time on the TOE with the NTP server’s date and time

4 Security Policy

4.1 Security audit

The Cisco X-ES Xpedite5205 Embedded Services Router provide extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco ESR routers generate an audit record for each auditable event. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. The administrator configures auditable events, backs-up, and manages audit data storage. The TOE provides the audit trail protection by providing remote backup to a syslog server over an encrypted channel. The audit messages include a timestamp that can be provided by the TOE or an optional NTP server in the operational environment.

4.2 Cryptographic support

The TOE provides cryptography in support of other Cisco ESR security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 2 (Certificate #2242). The TOE provides cryptography in support of VPN connections and remote administrative management via SSHv2.

4.3 Full residual information protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

4.4 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The IKE phase authentication for the IPsec communication channel between the TOE and authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules that includes special characters. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE optionally supports use of a RADIUS or TACACS+ AAA server (part of the IT Environment) to facilitate authentication (including single-use authentication, or password-based authentication) for administrative users attempting to connect to the TOE's CLI.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and SSH connections.

4.5 Security management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection. The TOE provides the ability to securely manage:

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE; and
- TOE configuration file storage and retrieval.

The TOE supports two separate administrative roles: non-privileged Administrator and privileged Administrator. Only the privileged administrator can perform all of the above security relevant management functions. The privileged Administrator is also considered to be the Authorized Administrator and Security Administrator.

Administrators can create configurable login banners to be displayed at time of login, and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

4.6 Packet Filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers as well as between remote VPN clients and the TOE. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map sets.

4.7 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally Cisco IOS is not a general-purpose operating system and access to Cisco IOS memory space is restricted to only Cisco IOS functions.

Use of separate VLANs is used to ensure routing protocol communications between the TOE and neighbor routers including routing table updates and neighbor router authentication will be logically isolated from traffic on other VLANs.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module. Whenever any system failures occur within the TOE the TOE will cease operation.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of malicious software.

4.8 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

4.9 Trusted Path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2, and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In

addition, IPsec is used to secure the session between the TOE and the authentication servers. The TOE can also establish trusted paths of peer-to-peer VPN tunnels. The peer-to-peer VPN tunnels can be used for securing the session between the TOE and authentication server/syslog server. In addition, the TOE can establish secure VPN tunnels with IPsec VPN clients. Remote VPN clients are able to securely connect into the X-ES over an encrypted session in order to connect to an authorized internal private network.

The TOE also supports direct connections from VPN clients, and protects against threats related to those client connections. The TOE disconnects sessions that have been idle too long, can be configured to deny sessions based on IP, time, and day, and can be configured to NAT external IPs of connecting VPN clients to internal network addresses.

5 Assumptions, Threats, and OSPs

5.1 Assumptions

The ST identifies the following assumptions about the use of the product:

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

5.2 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- User data may be inadvertently sent to a destination not intended by the original sender.

- Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions
- Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network
- Access to services made available by a protected network might be used counter to Operational Environment policies
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF
- If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver
- A malicious party attempts to change the data being sent – resulting in loss of integrity

5.3 Organizational Security Policies

The ST identifies the following organizational security policy that the TOE and its operational environment are intended to fulfill:

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.

6 Documentation

Cisco offers a number of guidance documents along with a CC-specific supplemental document describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

The vendor provided customer documentation for the TOE, which has been provided in the table below.

Table 4: Documentation

#	Title	Link
[1]	Cisco IOS IOS 15.2(4)GC Command Reference	http://www.cisco.com/en/US/products/ps11746/prod_command_reference_list.html
[2]	Installing Cisco IOS on the XPedite5205	http://www.cisco.com/en/US/docs/solutions/GGSG-Engineering/15_2_3GC/Install/X-ES_Instructions.pdf
[3]	Configuration Fundamentals Configuration Guide Cisco IOS Release 15MT	http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book.html
[4]	Network Management Configuration Guide Library, Cisco IOS Release 15M&T	http://www.cisco.com/en/US/docs/ios-xml/ios/net_mgmt/config_library/15-mt/netmgmt-15-mt-library.html
[5]	Securing User Services Configuration Guide Library, Cisco IOS Release 15M&T	http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/15-mt/secuser-15-mt-library.html
[6]	Loading and Managing System Images Configuration Guide, Cisco IOS Release 15M&T	http://www.cisco.com/en/US/docs/ios-xml/ios/sys-image-mgmt/configuration/15-mt/sysimgmgmt-15-mt-book.html
[7]	Technical Specifications of XPedite5205	http://www.xes-inc.com/products/view/xpedite5205/
[8]	XPedite5205 User Manual	N/A – Note: A login to the X-ES website is required to access the User Manual.

#	Title	Link
[9]	Software Configuration Guide for Cisco IOS Release 15.2(4)	http://www.cisco.com/en/US/products/ps11746/products_installation_and_configuration_guides_list.html
[10]	Secure Connectivity Configuration Guide Library, Cisco IOS Release 15M&T	http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/15-mt/secon-15-mt-library.html
[11]	Configuring Certificate Enrollment for a PKI	http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pki.pdf
[12]	Public Key Infrastructure Configuration Guide, Cisco IOS Release 15MT	http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book.html
[13]	Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS Release 15M&T	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book.html
[14]	Configuring Internet Key Exchange Version 2 (IKEv2)	http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/15-1mt/Configuring_Internet_Key_Exchange_Version_2.html

Any other customer documentation pertaining to the TOE was not evaluated and hence should not be relied upon for administration of the TOE in its evaluated configuration.

7 Product Testing

This section provides discussion of the testing effort performed against the TOE in this evaluation, as taken from the Cisco X-ES Xpedite5205 Common Criteria Test Report and Procedures documentation, dated October 28, 2014.

7.1 Evaluated Configuration

The TOE is Cisco X-ES Xpedite5205 Embedded Services Router which is installed and configured according to the X-ES Xpedite5205 Embedded Services Router Common Criteria Operational User Guidance and Preparative Procedures as well as the Installation Guide for the respective Cisco ESR router models included in the TOE. The configuration used during testing is the same as shown before in Figure 1: TOE Deployment Example.

7.1 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- Cisco X-ES Xpedite5205 Common Criteria Test Report and Procedures, Version 2.0, October 28 2014.

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST. The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in NDPP and VPNEP. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the CCTL location in Columbia, Maryland from April 2014 through November 2014.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for NDPP and VPNEP are fulfilled.

7.2 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC, the CEM, NDPP, VPNEP, and the CCEVS.

The results of the assurance requirements are summarized in this section. The details of the evaluation results are recorded in the Evaluation Technical Report (proprietary) and Test Summary Report provided by the CCTL. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 3.1 R4 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Network Devices Protection Profile (NDPP) and VPN Extended Package. The evaluation determined the X-ES Xpedite5205 TOE to be Part 2 extended, and meets the SARs contained the PP.

All assurance activities and work units received a passing verdict. The following components are taken from CC part 3:

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative user guidance
- ALC_CMC.1 Labeling of the TOE
- ALC_CMS.1 TOE CM coverage
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.1 Security objectives for the operational environment
- ASE_REQ.1 Stated security requirements
- ASE_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability analysis

8 Validator Comments/Recommendations

The validation team suggests that the consumer pay particular attention to the installation guidance to ensure the devices are placed into the evaluated configuration. In order to remain CC compliant, the device(s) must first be configured for FIPS mode.

As was noted in the Clarification of Scope section of this report, the devices provide more functionality than was covered by the evaluation. Only the functionality claimed in the SFR's in the Security Target was evaluated. All other functionality provided by the devices needs to be assessed separately and no further conclusions should be drawn as to their effectiveness, nor can any claims be made relative to their security based upon this evaluation.

The validators note that the Technical Decisions TD0015, TD0014, and TD0012 were applied to this evaluation. The Technical Decisions are available on the NIAP web site, but their impact on this evaluation is described below:

- TD0015: In the NDPP v1.1, FPF_RUL_EXT.1.7 Tests 4-6 refer to Table 9-1 (Defined Protocol-specific Values), which incorrectly identifies IPv6 Extension Header numbers as transport layer protocols. RFC 2460 lists the following IPv6 Extension Headers: Hop-by-Hop

options (0), Destination options (60), Routing (43), Fragment (44), AH (51), and ESP (50)). TD00015 states that the IPv6 extension header numbers do not need to be tested and these tests are not included in the evaluation.

- TD0014: For FCS_IPSEC_EXT.1.13 in the VPNEPv1.1, it is sufficient for the TOE to be configured to adhere to SFR and ensure cryptographic algorithm strength, i.e., configuration is equivalent to “default” cryptographic algorithm strength.
- TD0012: Algorithms not identified in FCS_SSH_EXT.1.4 must not be allowed in the evaluated configuration of the TOE; other cipher suites (such as 3DES-CBC) must be disabled in evaluated configurations. The Assurance Activities associated with this requirement must verify that connection attempts with algorithms not listed in FCS_SSH_EXT.1.4 are denied.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities prescribed in the NDPPv1.1 with Errata #2, the VPNEPv1.1, and the Technical Decisions listed above. Also, that the evaluation team correctly verified that the product meets the claims of the associated Security Target.

9 Annexes

Not applicable.

10 Security Target

X-ES Xpedite5205 Embedded Services Router Security Target, Version 1.0, October 13, 2014

11 Acronym List

CC	Common Criteria
CCTL	CC Testing Laboratory
CI	Configuration Item
CM	Configuration Management
CVE	Common Vulnerabilities and Exposures
FSP	Functional Specification
GUI	Graphical User Interface
ID	Identity/Identification
IP	Internet Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

12 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- [1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.
- [2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012
- [3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
- [4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.
- [5] X-ES Xpedite5205 Embedded Services Router Security Target, Version 1.0, October 13, 2014
- [6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.
- [7] Evaluation Technical Report For X-ES Xpedite5205 Embedded Services Router parts 1 and 2, version 1.0, April 2014.
- [8] Assurance Activities Report for X-ES Xpedite5205 Embedded Services Router, Version 1.1, 12 July 2014
- [9] X-ES Xpedite5205 Common Criteria Test Report and Procedures, Version 2.0, October 28, 2014