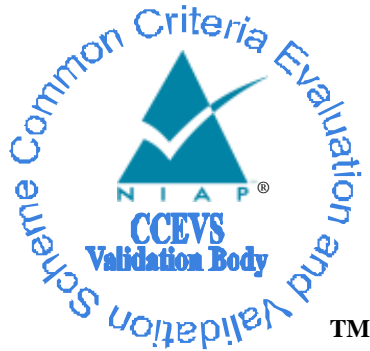


**National Information Assurance Partnership**  
**Common Criteria Evaluation and Validation Scheme**



**Validation Report**

**for**

**Cisco Integrated Services Router 4400 Series**

**(ISR-4400)**

**Report Number:** CCEVS-VR-VID10600-2015  
**Dated:** February 12, 2015  
**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

VALIDATION REPORT  
Cisco ISR-4400

**ACKNOWLEDGEMENTS**

**Validation Team**

Jerome Myers  
Luke Florer  
*The Aerospace Corporation*

**Common Criteria Testing Laboratory**

Kevin Micciche  
Kevin Steiner  
Gregory Beaver  
  
*Leidos (formerly SAIC, Inc.)  
Columbia, MD*

## Table of Contents

1	Executive Summary .....	1
2	Identification .....	4
2.1	Threats.....	4
2.2	Organizational Security Policies.....	5
3	Architectural Information .....	6
4	Assumptions.....	8
4.1	Clarification of Scope .....	8
5	Security Policy .....	10
5.1	Security Audit .....	10
5.2	Cryptographic Support.....	10
5.3	Full Residual Data Protection .....	10
5.4	Identification and Authentication .....	10
5.5	Security Management .....	11
5.6	Packet Filtering .....	11
5.7	Protection of the TSF .....	11
5.8	TOE Access .....	11
5.9	Trusted Path/Channels .....	12
6	Documentation .....	13
7	Independent Testing.....	15
8	Evaluated Configuration .....	16
9	Results of the Evaluation .....	17
10	Validator Comments/Recommendations .....	18
11	Annexes 19	
12	Security Target.....	20
13	Abbreviations and Acronyms .....	21
14	Bibliography .....	23

## List of Tables

Table 1: Router Model in the Evaluated Configuration .....	2
Table 2: Evaluation Details.....	2
Table 3: ST and TOE Identification.....	4
Table 4: Supporting TOE Guidance Documentation.....	13
Table 5: TOE Security Assurance Requirements .....	17

## 1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Cisco Integrated Services Router 4400 Series (hereafter referenced as Cisco ISR-4400). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

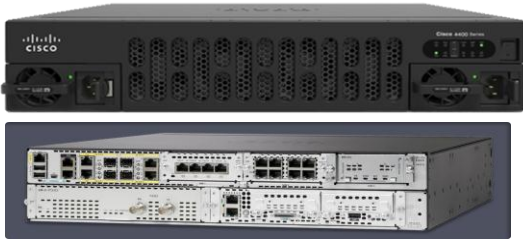

The evaluation of Cisco ISR-4400 was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in February 2015. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013 (VPNEPv1.1). The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site ([www.niap-ccevs.org](http://www.niap-ccevs.org)).

The Leidos evaluation team determined that Cisco ISR-4400 is conformant to the claimed Protection Profiles (PPs) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Leidos evaluation team.

The TOE is a hardware and software solution that consists of the Universal Cisco Inter-network Operating System (IOS) software image Release XE 3.13.0 running on the hardware listed in Table 1. The network on which it resides is considered part of the operational environment.

VALIDATION REPORT  
Cisco ISR-4400

**Table 1: Router Model in the Evaluated Configuration**

Hardware	Picture	Size	Interfaces
Cisco 4451-X ISR		3.5 x 17.25 x 18.5 in.	(4) onboard WAN or LAN 10/100/1000 ports (4) RJ-45 based ports (4) SFP-based ports (2) Enhanced service- module slots (2) Double wide service- module slots (3) NIM slots (1) onboard ISC slot (2) External USB 2.0 slots (type A) (1) USB console port (type B) (1) Serial console port (1) Serial auxiliary port
Cisco 4431-X ISR		1.73 x 17.25 x 19.97 in.	(4) onboard WAN or LAN 10/100/1000 ports (4) RJ-45 based ports (4) SFP-based ports (3) NIM slots (1) onboard ISC slot (2) External USB 2.0 slots (type A) (1) USB console port (type B) (1) Serial console port (1) Serial auxiliary port

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the ST. 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.

**Table 2: Evaluation Details**

Item	Identifier
Evaluated Product	Cisco Integrated Services Router 4400 Series

VALIDATION REPORT  
Cisco ISR-4400

<b>Item</b>	<b>Identifier</b>
<b>Sponsor &amp; Developer</b>	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134
<b>CCTL</b>	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
<b>Completion Date</b>	February 2015
<b>CC</b>	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
<b>Interpretations</b>	There were no applicable interpretations used for this evaluation.
<b>CEM</b>	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
<b>PP</b>	<i>Protection Profile for Network Devices</i> , Version 1.1, 8 June 2012 <i>Network Device Protection Profile (NDPP) Extended Package VPN Gateway</i> , Version 1.1, 12 April 2013 <i>Security Requirements for Network Devices Errata #2</i> , 13 January 2014
<b>Evaluation Class</b>	None
<b>Disclaimer</b>	The information contained in this Validation Report is not an endorsement of the Cisco ISR-4400 by any agency of the U.S. Government and no warranty of Cisco ISR-4400 is either expressed or implied.
<b>Evaluation Personnel</b>	Kevin Micciche Kevin Steiner Gregory Beaver
<b>Validation Personnel</b>	Jerome Myers Luke Florer

## 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) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

**Table 3: ST and TOE Identification**

Name	Description
ST Title	Cisco Integrated Services Routers (ISR) 4400 Series
ST Version	0.5
Publication Date	January 28, 2015
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Integrated Services Routers (ISR) 4400 Series
TOE Hardware Models	Cisco 4451-X, Cisco 4431-X
TOE Software Version	Internetwork Operating System (IOS) XE 3.13.0
Keywords	Router, Data Protection, Authentication

### 2.1 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.



VALIDATION REPORT  
Cisco ISR-4400

- 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

## **2.2 Organizational Security Policies**

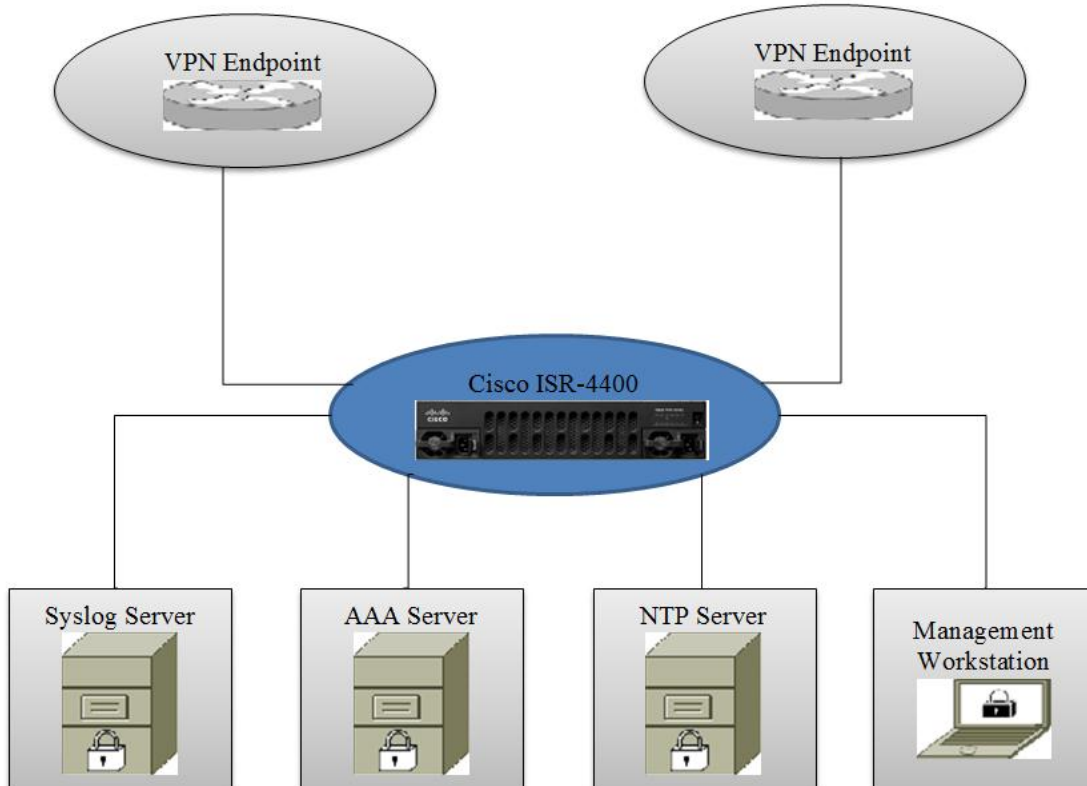
The ST identifies the following organizational security policy that the TOE and its operational environment are intended to fulfill:

- 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.

### 3 Architectural Information

The TOE consists of one or more physical devices of the Cisco 4400 Series ISRs and includes the Cisco IOS-XE software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination. IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IP sec, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE802.1ag, and IEEE802.3ah protocols are supported on the ISR-4400 model.

The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the TOE is to be remotely administered, then the management station must be connected to an internal network, SSHv2 must be used to connect to the switch. A syslog server is also used to store audit records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.



VALIDATION REPORT  
Cisco ISR-4400

Figure 1 depicts an example TOE deployment.

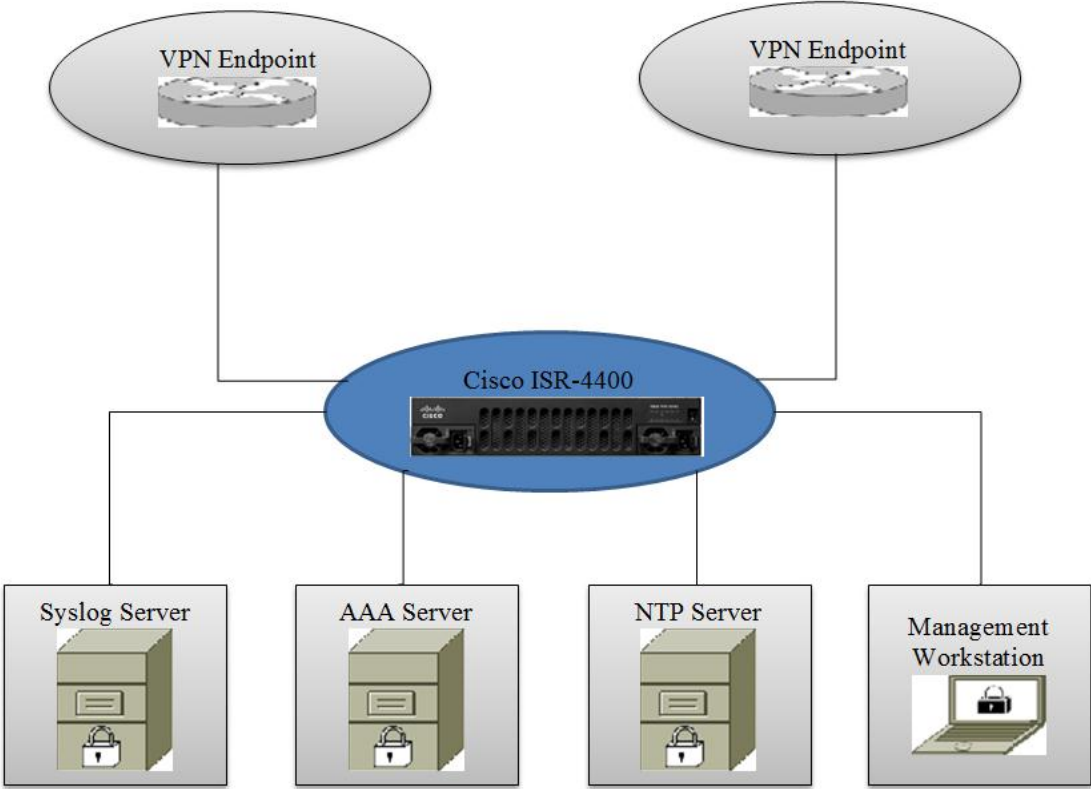


Figure 1: TOE Deployment Example

## 4 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.

### 4.1 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 specific product capabilities are excluded from use in the evaluated configuration:
  - a. Non-FIPS 140-2 mode of operation—this mode of operation allows cryptographic operations that are not FIPS-approved
  - b. Telnet—this service must be disabled in the evaluated configuration
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

VALIDATION REPORT  
Cisco ISR-4400

- 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

## 5 Security Policy

The TOE enforces the following security policies as described in the ST.

### 5.1 Security Audit

The Cisco ISR-4400 provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco ISR-4400 generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the audit trail protection by providing remote backup to a syslog server over an encrypted channel.

### 5.2 Cryptographic Support

The TOE provides cryptography in support of other Cisco ISR-4400 security functionality. The cryptographic algorithms implemented in support of this functionality have been NIST-validated and the relevant Cryptographic Algorithm Validation Program (CAVP) certificate numbers are listed in Table 6 of the ST. The TOE provides cryptography in support of VPN connections and remote administrative management via SSHv2. The cryptographic services provided by the TOE are: Internet Key Exchange, Secure Shell Establishment, RSA/DSA Signature Services, SP 800-90 RBG, SHS, and AES.

The TOE can also use the X.509v3 certificate for securing IPsec and SSH sessions.

### 5.3 Full Residual Data Protection

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

### 5.4 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. 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) for authentication of administrative users attempting to connect to the TOE's CLI.

The TOE provides an automatic lockout when a user attempts to authenticate and enters invalid information. After a defined number of authentication attempts fail exceeding the configured allowable attempts, the user is locked out until an authorized administrator can enable the user account.

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

## 5.5 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 administrator roles: non-privileged administrator and privileged administrator. Only the privileged administrator can perform the above security relevant management functions.

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.

## 5.6 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.

## 5.7 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-XE is not a general-purpose operating system and access to Cisco IOS-XE memory space is restricted to only Cisco IOS-XE functions.

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.

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.

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.

## 5.8 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.

VALIDATION REPORT  
Cisco ISR-4400

## **5.9 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 channels of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server.



VALIDATION REPORT  
Cisco ISR-4400

## 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 guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- Cisco ISR-4400 CC Configuration Guide, Version 0.4, November 5, 2014

This document in turn references the following documents that provide additional detailed guidance for specific TOE capabilities. Note that the evaluation examined these referenced documents only to the extent necessary to complete the assurance activities specified in the claimed PPs.

**Table 4: Supporting TOE Guidance Documentation**

Title	Link
Loading and Managing System Images Configuration Guide, Cisco IOS XE Release 3S	<a href="http://www.cisco.com/en/US/docs/ios-xml/ios/sys-image-mgmt/configuration/xe-3s/sysimgmgmt-xe-3s-book.html">http://www.cisco.com/en/US/docs/ios-xml/ios/sys-image-mgmt/configuration/xe-3s/sysimgmgmt-xe-3s-book.html</a>
Hardware Installation Guide for the Cisco 4400 Series Integrated Services Router	<a href="http://www.cisco.com/en/US/docs/routers/access/4400/hardware/installation/guide/C4400isr.pdf">http://www.cisco.com/en/US/docs/routers/access/4400/hardware/installation/guide/C4400isr.pdf</a>
Configuration Fundamentals Configuration Guide Cisco IOS XE Release 3S	<a href="http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/configuration/xe-3s/fundamentals-xe-3s-book.html">http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/configuration/xe-3s/fundamentals-xe-3s-book.html</a>
Network Management Configuration Guide Library	<a href="http://www.cisco.com/en/US/docs/ios-xml/ios/net_mgmt/config_library/xe-3s/netmgmt-xe-3s-library.html">http://www.cisco.com/en/US/docs/ios-xml/ios/net_mgmt/config_library/xe-3s/netmgmt-xe-3s-library.html</a>
Securing User Services Configuration Guide Library, Cisco IOS XE Release 3S	<a href="http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3s/secuser-xe-3s-library.html">http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3s/secuser-xe-3s-library.html</a>
Using Setup Mode to Configure a Cisco Networking Device	<a href="http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_setup.html">http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_setup.html</a>
Cisco ISR-4400 FIPS 140-2 Non-proprietary Security Policy	NIST CMVP Certificate #2278 at <a href="http://csrc.nist.gov/groups/STM/cmvp">http://csrc.nist.gov/groups/STM/cmvp</a>
Cisco IOS Security Command Reference	<a href="http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html">http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html</a> <a href="http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-d1-cr-book.html">http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-d1-cr-book.html</a> <a href="http://www.cisco.com/en/US/docs/ios-xml/ios/security/m1/sec-m1-cr-book.html">http://www.cisco.com/en/US/docs/ios-xml/ios/security/m1/sec-m1-cr-book.html</a> <a href="http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html">http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html</a>
Configuring Certificate Enrollment for a PKI	<a href="http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pki.pdf">http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pki.pdf</a>

VALIDATION REPORT  
Cisco ISR-4400

Title	Link
Public Key Infrastructure Configuration Guide, Cisco IOS XE Release 3S	<a href="http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/xe-3s/sec-pki-xe-3s-book.pdf">http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/xe-3s/sec-pki-xe-3s-book.pdf</a>
Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS XE Release 3S	<a href="http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book.pdf">http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book.pdf</a>
Configuring Internet Key Exchange Version 2 (IKEv2)	<a href="http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-cfg-ikev2-flex.html">http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-cfg-ikev2-flex.html</a>
Cisco IOS Configuration Fundamentals Command Reference	<a href="http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/Cisco_IOS_Configuration_Fundamentals_Command_Reference.html">http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/Cisco_IOS_Configuration_Fundamentals_Command_Reference.html</a>

The above documents are considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

The Security Target used is:

- Cisco Integrated Services Routers (ISR) 4400 Series Security Target, Version 0.5, January 28, 2015

## 7 Independent Testing

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

- Cisco Integrated Service Routers 4400 Series (ISR) Common Criteria Test Report and Procedures, Version 1.0, December 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 for a product claiming conformance to NDPPv1.1 with ERRATA #2 and VPNEPv1.1.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in NDPPv1.1 with ERRATA #2 and VPNEPv1.1. 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 November 2014 through December 2014.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE (in three distinct but representative configurations) 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 NDPPv1.1 with ERRATA #2 and VPNEPv1.1 are fulfilled.

## **8 Evaluated Configuration**

The evaluated version of the TOE is Cisco ISR 4451-X and Cisco ISR 4431-X running IOS XE 3.13.0, as installed and configured according to the Cisco ISR-4400 CC Configuration Guide as well as the supporting guidance documentation identified in Table 4.

## 9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 with ERRATA #2 and in Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

**Table 5: TOE Security Assurance Requirements**

<b>Assurance Component ID</b>	<b>Assurance Component Name</b>
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

## 10 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 and Telnet must be disabled. Also, device administrators should ensure that all access controls lists (ACLs) contain a final rule to drop all unmatched traffic.

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 TOE claims conformance to the NDPP v1.1 with Errata #2.

The validators note that the Technical Decisions TD0019, 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:

- TD0019: For TOEs claiming conformance to both the NDPP v1.1 with Errata #2 and the VPN Gateway EP V1.1, the FTP\_ITC.1 and FTP\_TRP.1 requirements in NDPP v1.1 can be updated by removing the data channel modification tests, along with the removal of the specified test requirements in FPT\_ITT.1. The result is the elimination of the following tests from ND PP V1.1: FTP\_ITC.1: Test 4, FTP\_TRP.1: Test 4, and FPT\_ITT.1: Test 3. These test were not included in the evaluation.
- 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.

## **11 Annexes**

Not applicable.

## **12 Security Target**

Cisco Integrated Services Routers (ISR) 4400 Series Security Target, version 0.5, January 28, 2015



## 13 Abbreviations and Acronyms

<b>AAA</b>	Authentication, Authorization and Accounting
<b>AAR</b>	Assurance Activities Report
<b>CAVP</b>	Cryptographic Algorithm Validation Program
<b>CC</b>	Common Criteria
<b>CCEVS</b>	Common Criteria Evaluation and Validation Scheme
<b>CCTL</b>	CC Testing Laboratory
<b>CEM</b>	Common Methodology for IT Security Evaluation
<b>CLI</b>	Command Line Interface
<b>EP</b>	Extended Package
<b>ESP</b>	Encapsulating Security Payload
<b>ETR</b>	Evaluation Technical Report
<b>FIPS</b>	Federal Information Processing Standard
<b>IKE</b>	Internet Key Exchange
<b>IOS</b>	Inter-network Operating System
<b>IPsec</b>	Internet Protocol security
<b>ISR</b>	Integrated Service Router
<b>IT</b>	Information Technology
<b>LAN</b>	Local Area Network
<b>NDPP</b>	Network Device Protection Profile
<b>NIAP</b>	National Information Assurance Partnership
<b>NIM</b>	Network Interface Module
<b>NIST</b>	National Institute of Standards and Technology
<b>NSA</b>	National Security Agency
<b>NTP</b>	Network Time Protocol
<b>NVLAP</b>	National Voluntary Laboratory Assessment Program
<b>OS</b>	Operating System
<b>PCL</b>	Product Compliant List
<b>PP</b>	Protection Profile
<b>RADIUS</b>	Remote Authentication Dial In User Service
<b>RFC</b>	Request For Comment
<b>SA</b>	Security Association
<b>SAR</b>	Security Assurance Requirement
<b>SFP</b>	Small Form-factor Pluggable
<b>SFR</b>	Security Functional Requirement
<b>SNMP</b>	Simple Network Management Protocol
<b>SSHv2</b>	Secure Shell version 2
<b>SSL</b>	Secure Sockets Layer
<b>ST</b>	Security Target
<b>TACACS+</b>	Terminal Access Controller Access-Control System Plus
<b>TLS</b>	Transport Layer Security
<b>TOE</b>	Target of Evaluation
<b>TSF</b>	TOE Security Functions
<b>TSS</b>	TOE Summary Specification
<b>USB</b>	Universal Serial Bus
<b>VPN</b>	Virtual Private Network
<b>VR</b>	Validation Report

VALIDATION REPORT  
Cisco ISR-4400

**WAN**      Wide Area Network

## 14 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] Cisco Integrated Services Routers (ISR) 4400 Series Security Target, version 0.5, January 28, 2015
- [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 Cisco Integrated Services Routers (ISR) 4400 Series (and associated AAR and test report), version 1.1, August 6, 2014.