# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme


TM

# Validation Report

# for

# Cisco 5921 Embedded Services Router

**Report Number:** CCEVS-VR-VID10586-2015
**Dated:** June 26, 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**

# ACKNOWLEDGEMENTS

## Validation Team

**Jerome Myers**
***The Aerospace Corporation***

**Jean Petty**
***The MITRE Corporation***

## Common Criteria Testing Laboratory

***Leidos Inc. (formerly SAIC, Inc.)***
***Columbia, MD***

# Table of Contents



# List of Tables

# 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 for 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 tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read 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 the Cisco 5921 Embedded Services Router (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the 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 documented in the ST.

The evaluation of the Cisco 5921 Embedded Services Router was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in January 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, and assurance activities specified in *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, v1.4, 21 Oct 2013. 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).

The TOE is a software-only solution for protecting the network. The focus of this evaluation was on the IPsec Virtual Private Network (VPN) client functionality of the TOE. It supports VPN client session capabilities that provide secure tunnels to authenticated remote endpoints or gateways. The TOE encrypts all information that flows between itself and its VPN gateway or IPsec peer. The TOE software consists of the Universal Cisco IOS software image Release IOS 15.5(2)T. The TOE requires the following components in its operational environment:

- An x86 processor with a minimum 256 MB of memory
- Linux Kernel 2.6.32 or later.

The Leidos evaluation team determined that the TOE is conformant to *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, v1.4, 21 Oct 2013. The TOE, when configured as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in *Cisco 5921 Embedded Services Router Security Target*, Version 1.0, April 9, 2014. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test reports produced by the Leidos evaluation team.

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test reports. The validation team found that the evaluation showed that the TOE satisfies all of the security functional and assurance requirements stated in the Security Target (ST). The evaluation also showed that the TOE is conformant to *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, v1.4, 21 Oct 2013, and that the assurance activities specified in the Protection Profile had been performed appropriately. 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.

## 1.1 Interpretations

Not applicable.

## 1.2 Threats

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

- Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data. 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.
- User data may be inadvertently sent to a destination not intended by the original sender because it is not rendered inaccessible after it is done being used.

# 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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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).

Table 1 provides information needed to completely identify the product and its evaluation.

**Table 1: Evaluation Details**

| | |
|---|---|
| **Evaluated Product:** | Cisco 5921 Embedded Services Router (ESR) running IOS 15.5(2)T |
| **Sponsor:** | Cisco Systems, Inc.<br>170 West Tasman Dr.<br>San Jose, CA 95134 |
| **Developer:** | Cisco Systems, Inc.<br>170 West Tasman Dr.<br>San Jose, CA 95134 |
| **CCTL:** | Leidos (formerly Science Applications International Corporation)<br>6841 Benjamin Franklin Drive<br>Columbia, MD 21046 |
| **Kickoff Date:** | 8 Jan 2015 |
| **Completion Date:** | 30 Jan 2015 |
| **CC:** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. |
| **Interpretations:** | None |
| **CEM:** | Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 3, July 2009. |
| **Evaluation Class:** | None |
| **PP:** | Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013 |
| **Evaluation Personnel:** | Leidos (formerly Science Applications International Corporation):<br>Anthony J. Apted<br>Greg Beaver<br>Dawn Campbell<br>Pascal Patin |
| **Validation Body:** | National Information Assurance Partnership CCEVS |

# 3 Security Policy

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

**Note:** Much of the description of the security policy has been derived from the Cisco 5921 Embedded Services Router Security Target and Final Evaluation Technical Report (ETR).

## 3.1 Cryptographic Support

The TOE includes NIST-validated cryptographic algorithms that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of IPsec connections. In addition, the TOE can use X.509v3 certificates for authenticating IPsec sessions. Note that in order to be in the evaluated configuration, the TOE must be configured in FIPS mode, which ensures the TOE's configuration is consistent with the FIPS 140-2 standard.

## 3.2 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 zeroes. Residual data is never transmitted from the TOE.

## 3.3 Identification and Authentication

The TOE performs device-level authentication of the remote device (IPsec peer or VPN Gateway). 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 TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec sessions.

## 3.4 Security Management

The TOE provides all the capabilities necessary to securely manage the TOE. The administrative user can connect to the TOE using the CLI to perform these functions via SSH or at the local console. All of these functions can be performed via the CLI either locally or remotely.

The specific evaluated management capabilities provided by the TOE are:

- Configuration of IKE protocol version(s) used
- Configuration of IKE authentication techniques used
- Configuration of the session key lifetimes
- Configuration of the certificate revocation check
- Specification of the algorithm suites that may be proposed and accepted during the IPsec exchanges
- Loading of X.509v3 certificates used by the security functions of the TOE
- Ability to update the TOE, and to verify TOE updates
- Specification of the VPN gateways to use for connections
- Specification of the client credentials to be used for connections
- Ability to accept or deny the validity of a certificate.

The client credentials can be a client X.509 certificate and/or pre-shared key that are used for authentication to the VPN Gateway.

## 3.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by providing a complete implementation of the Cisco IOS software. Additionally, the TOE performs testing to verify correct operation of the TOE and of its 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.

## 3.6 Trusted Channels

The TOE initiates IPsec tunnels with remote IPsec peers and VPN Gateways.

# 4 Assumptions and Clarification of Scope

## 4.1 Assumptions

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

- Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

## 4.2 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 *Protection Profile for IPsec Virtual Private Network (VPN) Clients* and performed by the evaluation team).
2. This evaluation covers only the specific 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 *Cisco 5921 Embedded Services Router Security Target*, Version 1.0, June 22, 2015. 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 TOE relies on its operational environment as follows:
    a. The TOE operates on an underlying OS and requires Linux Kernel 2.6.32 or later.
    b. The TOE and its underlying OS in turn operate on an underlying hardware platform and require an x86 processor with a minimum of 256 MB of memory.
    c. The evaluated IPsec VPN Client functionality of the TOE requires the presence in the operational environment of an IPsec Peer or a VPN Gateway with which the TOE can establish a secure IPsec session.
6. The TOE optionally supports the following components in its operational environment:
    a. Certification Authority, from which the TOE can request a valid certificate during certificate enrollment.
    b. Local console—any console device directly connected to the underlying hardware platform via a serial console port, which provides the administrator access to the TOE's CLI.

c. Management workstation with SSH client—any workstation device, with an SSH client installed, connected to the underlying hardware platform via a network management port, which provides the administrator secure remote access to the TOE's CLI via SSH.

d. NTP server—the TOE supports communications with an NTP server for synchronization of its internal clock.

e. USB token—the TOE supports the optional storing of digital certificates and private keys on a USB token. The token can securely store any type of file within its available storage space (32 KB). Configuration files that are stored on the USB token can be encrypted and accessed only via a user PIN. The device does not load the configuration file unless the proper PIN has been configured for secure deployment of device configuration files.

7. The following product capabilities described in the product guidance documentation are outside the scope of this evaluation and so have not been subject to testing by the evaluation team:

   a. Generation of audit records

   b. Use of NTP

   c. Use of SSH

   d. Administrator identification and authentication (local and remote) and administrative roles

   e. Password complexity

   f. Login banners.

8. The TOE must be configured as described in *Cisco 5921 Embedded Services Router Common Criteria Operational User Guidance And Preparative Procedures*, Version 1.0, June 22, 2015, to be in the evaluated configuration.

# 5 Architectural Information

The TOE is the Cisco 5921 Embedded Services Router (ESR) running IOS 15.5(2)T. It is an application designed to operate on small, low power Linux-based platforms with x86 processors. It is optimized for mobile and embedded networks that require IP routing and services. It can provide secure data, voice, and video communications to stationary and mobile network nodes across wired and wireless links. The focus of this evaluation is on its VPN client functionality.

The TOE supports VPN client session capabilities that provide secure tunnels to authenticated remote endpoints or gateways. The TOE is a FIPS 140-2 validated cryptomodule (Certificate #2244) that uses IPsec to protect all information that flows between itself and its VPN gateway or IPsec peer.

The TOE is a software-only Linux application. The underlying operating system and hardware, and the network on which they reside, are considered part of the TOE operational environment.

# 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 primary guidance documentation for the TOE is:

- Cisco 5921 Embedded Services Router Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0, June 22, 2015

Section 1.3 of the above document references the following additional documents for supporting information, and provides URLs for accessing the current on-line releases:

- Cisco IOS 15.5(2)T Command Reference
- Cisco 5921 Embedded Services Router Integration Guide, Current Release: September 2013
- Configuration Fundamentals Configuration Guide Cisco IOS Release 15M&T
- Network Management Configuration Guide Library, Cisco IOS Release 15M&T
- Securing User Services Configuration Guide Library, Cisco IOS Release 15M&T
- Loading and Managing System Images Configuration Guide, Cisco IOS Release 15M&T
- IP Routing Configuration Guides
- Secure Connectivity Configuration Guide Library, Cisco IOS Release 15M&T
- Configuring Internet Key Exchange Version 2 (IKEv2).

# 7 IT Product Testing

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

- Cisco 5921 Common Criteria Test Report, Version 1.0, 20 January 2015

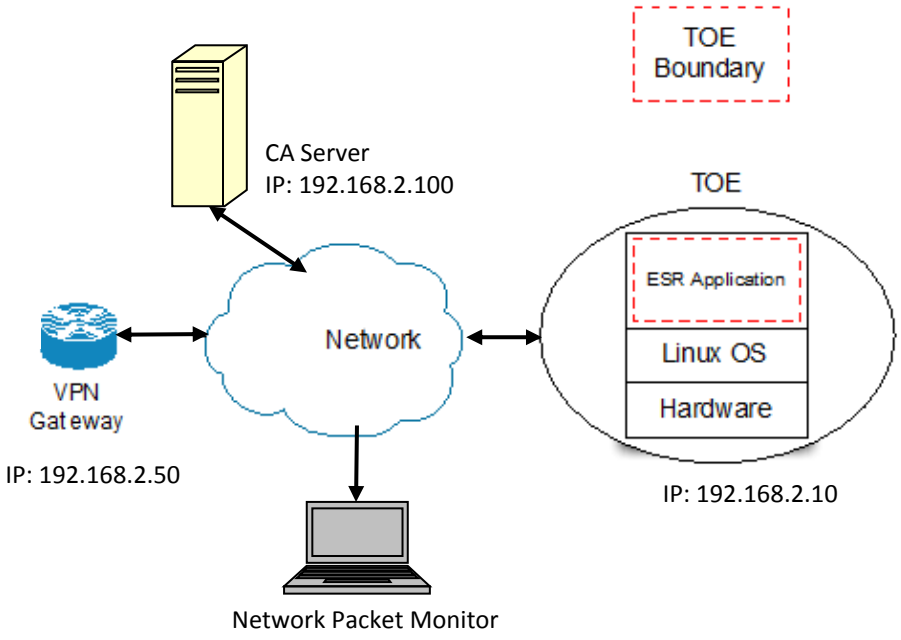
## 7.1 Developer Testing

The assurance activities in *Protection Profile for IPsec Virtual Private Network (VPN) Clients* do not specify any requirement for developer testing of the TOE.

## 7.2 Evaluation Team Independent Testing

The evaluation team devised a test plan based on the Test Assurance Activities specified in *Protection Profile for IPsec Virtual Private Network (VPN) Clients*. 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 identified above.

The test configuration is shown below:




As documented in the diagram above, the following hardware and software components were included in the evaluated configuration during testing:

- TOE Software
  - Cisco IOS 15.5(2)T
- TOE Hardware Platform
  - Intel Desktop board D2500CC, incorporating Intel Atom processor D2500 (refer to: http://www.intel.com/content/www/us/en/motherboards/desktop-motherboards/desktop-board-d2500cc.html)
- TOE Software Platform
  - CentOS 2.6.32-279.22

- Test Environment Components
  - Certificate Authority server
  - VPN Gateway
  - Network Packet Monitor

As can be seen above, the configuration used during testing of the TOE matches the configuration specified in the ST.

Evaluation testing took place at the Leidos CCTL facility in Columbia, Maryland in August and September 2014.

The vendor provided a specimen hardware platform as described above, with CentOS pre-installed. The evaluation team followed the installation and configuration procedures documented in the product guidance to install the TOE in the test environment.

Subsequently, the evaluators exercised all the test cases. The tests were selected in order to ensure that each of the test assertions specified in *Protection Profile for IPsec Virtual Private Network (VPN) Clients* were covered. All tests passed. A summary of the testing performed by the evaluation team is provided in *Cisco 5921 Embedded Services Router Common Criteria Assurance Activities Report*.

## 7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration.

# 8 Evaluated Configuration

The TOE is Cisco 5921 Embedded Services Router running IOS 15.5(2)T, which is installed and configured according to *Cisco 5921 Embedded Services Router Common Criteria Operational User Guidance And Preparative Procedures*. The TOE in its evaluated configuration is installed on a hardware platform with an x86 processor and a minimum 256 MB of memory running Linux Kernel 2.6.32 or later. The TOE is configured to operate in FIPS mode.

# 9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, in conjunction with Version 3.1, Revision 3 of the CC and CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

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 in the PP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Final ETR, which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

**Table 2: Evaluated Assurance Requirements**

| Assurance Component ID | Assurance Component Name |
|---|---|
| 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 validators suggest that the consumer pay special attention to the evaluated configuration of the device(s), particularly the operating system platforms used by the TOE and the specific functionality defined within the Security Target.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Only the functionality implemented by the security functional requirements within the Security Target was evaluated. Other functionality included in the product was not assessed as part of this evaluation.

The product contains more functionality than was covered by the evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

# 11 Annexes

Not applicable.

# 12 Security Target

The ST for this product's evaluation is Cisco 5921 Embedded Services Router Security Target, Version 1.0, June 22, 2015.

# 13 Abbreviations and Acronyms

| | |
|---|---|
| AAR | Assurance Activities Report |
| CC | Common Criteria for Information Technology Security Evaluation |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCTL | Common Criteria Testing Laboratory |
| CEM | Common Evaluation Methodology for Information Technology Security |
| CLI | Command Line Interface |
| CM | Configuration Management |
| ESR | Embedded Services Router |
| ETR | Evaluation Technical Report |
| FIPS | Federal Information Processing Standard |
| IKE | Internet Key Exchange—a protocol used to set up a security association (SA) in the IPsec protocol suite |
| IP | Internet Protocol—communications protocol for relaying datagrams across network boundaries |
| IPsec | Internet Protocol Security—a protocol suite for securing IP communications |
| IT | Information Technology |
| MB | Megabyte |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NTP | Network Time Protocol—a means of synchronizing clocks over a computer network |
| NVLAP | National Voluntary Laboratory Assessment Program |
| PCL | Product Compliant List |
| PIN | Personal Identification Number—a password used to access a secured system (e.g., USB token) |
| RFC | Request for Comments—an Internet Engineering Task Force memorandum on Internet standards and protocols |
| SSH | Secure Shell—a network protocol for secure data communication and remote command execution |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| URL | Uniform Resource Locator—typically a web address |
| USB | Universal Serial Bus—a standard defining the cables, connectors and communications protocols used in a bus for connection, communication, and power supply between computers and electronic devices |
| USB token | A smart card with a USB interface |
| VPN | Virtual Private Network |
| VR | Validation Report |

# 14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Part 1: Introduction and general model. CCMB-2009-07-001.

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Part 2: Security functional components. CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. Part 3: Security assurance components. CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Evaluation methodology. CCMB-2009-07-004.

[5] Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013.

[6] Cisco 5921 Embedded Services Router Security Target, Version 1.0, January 20, 2015.

[7] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[8] Evaluation Technical Report for Cisco 5921 Embedded Services Router, Parts 1 and 2 (and associated AAR and Test Report), Version 1.0, 20 January 2015.