National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Cisco 7600 Series Router

Report Number: CCEVS-VR-VID10494-2012
Dated: 21 December 2012
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

Mike Allen (Lead Validator)
Jandria Alexander (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Gary Grainger
James Arnold
Tammy Compton
Julie Cowan
Chris Keenan
Science Applications International Corporation
Columbia, Maryland

Table of Contents

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 both 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 are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco 7600 Series Routers. It presents the evaluation results, their justifications, and the conformance results. This Validation Report 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 Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Cisco 7600 Series Routers was performed by the Science Applications International Corporation (SAIC), the Common Criteria Testing Laboratory, in Columbia, Maryland USA and was completed in November 2012.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Cisco Systems Inc. The ETR and test report used in developing this validation report were written by SAIC. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, dated July 2009 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 and ALC_DVS.1. The Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 3, dated July 2009 was used for this evaluation. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the Cisco 7600 Series Routers Security Target. The evaluation team determined the product to be both Part 2 extended and Part 3 augmented compliant, and meets the assurance requirements of EAL 2 augmented by ALC_FLR.2 and ALC_DVS.1. All security functional requirements are derived from Part 2 of the Common Criteria.

The Target of Evaluation (TOE) is a hardware configuration in Cisco 7600 Series of routers running IOS 15.1(3)S3 software. The evaluate hardware configurations consist of:

- One or more 7600 series chassis (7613, 7609-S, 7606-S, 7604 or 7603-S),
- One or more RSP720 Management Cards per chassis,
- One or more compatible line cards as identified in the Security Target.
- One VPN IPSec SPA (ws-ipsec-3) Line Card per Chassis

1.1 Interpretations

There are no applicable Common Criteria interpretations.

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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (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 Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant (if any); and
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Cisco 7600 Series Routers
Protection Profiles	None.
Security Target	*Cisco 7600 Series Routers Security Target*, Revision 0.13, November 27, 2012
Dates of evaluation	January 2012 through November 2012
Evaluation Technical Report	*Evaluation Technical Report for the Cisco 7600 Series Routers Part 1 (Non-Proprietary)*, Version 1.0, October 1, 2012 and *Evaluation Technical Report for the Cisco 7600 Series Routers Part 2 (Proprietary)*, Version 2.0, October 1, 2012
Conformance Result	Part 2 extended conformant and EAL2 Part 3 augmented with ALC_FLR.2 and ALC_DVS.1
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009 and all applicable NIAP and International Interpretations effective on January 19, 2012
Common Evaluation Methodology (CEM) version	CEM version 3.1R3 dated July2009and all applicable NIAP and International Interpretations effective on January 19, 2012
Sponsor	Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134
Developer	Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134
Common Criteria Testing Lab	Science Applications International Corporation, Columbia, MD 21045
Evaluators	Gary Grainger, James Arnold, Tammy Compton, Julie Cowan and Chris Keenan
Validation Team	Jandria Alexander and Mike Allen of the Aerospace Corporation

3 Security Policy

This section summarizes the security functionality of the TOE:

1. Security Audit
2. Cryptographic Support
3. User Data Protection
4. Identification and Authentication
5. Secure Management
6. Protection of the TSF
7. TOE Access

3.1 Security Audit

The TOE generates audit messages that identify specific TOE operations. 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. Auditable events include: all use of the user identification mechanism; any use of the authentication mechanism; any change in the configuration of the TOE; any matching of packets to access control entries in access control lists (ACLs) when traversing the TOE; and any failure of a packet to match an ACL rule allowing traversal of the TOE. The TOE will write audit records to the local logging buffer by default and can be configured to send audit data via syslog to a remote audit server, or display on the CLI console. These audit messages include a timestamp that can be provided by the TOE or an optional NTP server in the operational environment.

3.2 Cryptographic Support

The TOE provides cryptography support for secure communications and protection of information when configured in FIPS mode. The crypto module is FIPS 140-2 SL2 compliant with certificate number 1621. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; cryptographic hashing using SHA1; keyed-hash message authentication using HMAC-SHA1, and IPSec for authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE also implements SSHv2 for secure remote administration.

The TOE delivers VPN connections to remote entities using IPSEC. The VPN process includes remote device authentication, negotiation of specific cryptographic parameters for the session, and providing a secure connection to and from the remote device. For inbound or outbound connections with external IT entities that are capable of supporting VPN (e.g., a VPN Peer), the TOE will establish a secure connection. For other inbound or outbound traffic a secure connection will not be established.

3.3 Traffic Filtering (ACLs)

ACLs control whether routed IP packets are forwarded or blocked at the TOE interfaces that have been configured with IP addresses. The TOE examines each frame and packet to determine whether to forward or drop it on the basis of the data in the ACLs applied to the interfaces to the

TOE. For those interfaces configured with Layer-3 addressing the ACLs can be configured to filter IP traffic using: the source address of the traffic; the destination address of the traffic; and the layer 3 and 4 protocol identifier. Use of ACLs also allows restriction of remote administration connectivity to specific interfaces of the TOE so that sessions will only be accepted from approved management station addresses pre-established by the administrator.

The TOE supports routing protocols including BGP, RIPv2, and OSPFv2 to maintain routing tables, or routing tables can be configured and maintained manually. The security of the routing protocols is beyond the scope of this evaluation. Refer to the preparative procedures and operational guidance for the most secure configuration of the supported routing protocols. Since routing tables are used to determine which egress ACL is applied, the authority to modify the routing tables is restricted to authenticated administrators, and authenticated neighbor routers.

The TOE also ensures that packets transmitted from the TOE do not contain residual information from previous packets. Packets that are not the required length use zeros for padding so that residual data from previous traffic is never transmitted from the TOE.

The TOE allows VLAN connections to/from remote entities. The TOE provides the ability to identify which VLAN is associated with the network traffic. The TOE then permits or denies the network traffic based on the VLANs configured on the received /destined interface. This policy is applied after the Firewall policy.

3.4 Identification and Authentication

The TOE performs authentication, using Cisco IOS platform authentication mechanisms, to authenticate access to user EXEC and privileged EXEC command modes. All users wanting to access TOE services are identified and authenticated prior to being allowed to use any of the services. Once a user attempts to access the management functionality of the TOE (via EXEC mode), the TOE prompts the user for a user name and password. Only after the administrative user presents the correct identification and authentication credentials will access to the TOE functionality be granted.

The TOE supports use of a remote AAA server (RADIUS and TACACS+) as the enforcement point for identifying and authenticating users, including login and password dialog, challenge and response, and messaging support. Encryption of the packet body is provided through the use of RADIUS (note RADIUS only encrypts the password within the packet body, while TACACS+ encrypts the entire packet body except the header).

The TOE can be configured to display an advisory banner when administrators log in and also to terminate administrator sessions after a configured period of inactivity.

The TOE also supports authentication of other routers using router authentication supported by BGP, RIPv2, and OSPFv2. Each of these protocols supports authentication by transmission of MD5-hashed password strings, which each neighbor router uses to authenticate other routers.

The TOE also performs device-level authentication of the remote device (VPN peers). 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 itself. Device-level authentication is performed via IKE v1/IPSec v3 mutual authentication.

3.5 Security Management

The TOE allows authorized administrators to add new administrators, create, modify, or delete configuration details such as interface parameters and ACLs, and to modify and set the time and date.

The TOE router platform maintains privileged and semi-privileged administrator roles. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15 (has all privileges on the box); and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. The term "authorized administrator" is used in this ST to refer to any user which has been assigned to a privilege level permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions.

The TOE also supports external IT entities. These external IT entities are peer routers that pass network control information (e.g., routing tables) to the TOE. Also included are any other VPN peers with whom the TOE exchanges information, including VPN clients and VPN gateways.

3.6 Protection of the TSF

The TOE provides secure transmission when TSF data is transmitted between separate parts of the TOE (encrypted sessions for remote administration (via SSHv2)). The TOE is also able to detect replay of information and/or operations. The detection applied to network packets that are terminated at the TOE, such as trusted communications between the administrators to TOE, IT entity (e.g., authentication server) to TOE. If replay is detected, the packets are discarded. In addition, the TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to TOE generated audit records. Alternatively, an NTP server can be used to synchronize the clock.

Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

3.7 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 a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

4 Assumptions and Clarification of Scope

The assumptions in the following paragraph were considered during the evaluation of the Cisco 7600 Series Routers.

4.1 Assumptions

- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error.
- Administrators will be trained to periodically review audit logs to identify sources of concern
- Personnel will be trained in the appropriate use of the TOE to ensure security.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- Copies of TOE configuration data including representations of authentication data maintained off the TOE in hard-copy or soft-copy will be kept confidential and access will be limited to authorized administrators. Audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic.
- The TOE will be able to function with the software and hardware of other router vendors on the network.

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 and how the TOE needs to be configured to ensure it operates in the evaluated configuration.

- The TOE must be operated in the FIPS 140-2 mode.
- The security of the routing protocols is beyond the scope of this evaluation. Refer to the preparative procedures and operational guidance for the most secure configuration of the supported routing protocols.
- Telnet sends authentication data in plain text. This feature is enabled by default and must be disabled in the evaluated configuration.
- SNMP does not enforce the required role privileges. This feature is disabled by default and should not be configured for use in the evaluated configuration.

- HTTP Server for web user interface management: Sends authentication data in plain text and does not enforce the required role privileges. Not including this feature does not interfere with the management of TOE as defined in the Security Target.
- IEEE 802.11 Wireless Standards: The evaluated configuration of 7600 Routers as described is the Security Target does not support implementing wireless local area network. Use of this feature requires additional hardware beyond what is included in the evaluated configuration.
- MAC address filtering: The SFPs in the Security Target are defined as information flow polices, not as access polices that allow access based on MAC address.
- Flexible NetFlow used for traffic analysis and optimization, does not include performance/optimization features and should not be used in the evaluated configuration. Not including this feature does not interfere with the enforcement of the security policies as defined in the Security Target.
- The Network Assistant application and CiscoWorks LAN Management Solutions are separately licensed, separate products and are not included in the scope of this evaluation.

5 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

A Cisco 7600 Series Router is a routing platform used to construct IP networks by interconnecting multiple smaller networks or network segments. As a Layer3 router, it supports routing of traffic based on tables identifying available routes, conditions, distance, and costs to determine the best route for a given packet. Routing protocols used by the TOE include BGP, RIPv2, and OSPFv2.

5.1 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 2 - IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
NTP Server	No	The TOE supports communications with an NTP server to receive clock updates.
Syslog Server	No	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.
Authentication Server	No	The authentication server (RADIUS and TACACS+) is used to provide centralized authentication and related auditing for one or more distributed instances of the TOE.

5.2 TOE Description

This section provides an overview of the Cisco 7600 Series Routers Target of Evaluation (TOE). The TOE is comprised of one or more 7600 chassis containing compatible line cards and RSP720 Management Cards running IOS 15.1(3)S3.

5.3 TOE Evaluated Configuration

Table 3 - Evaluated Configurations

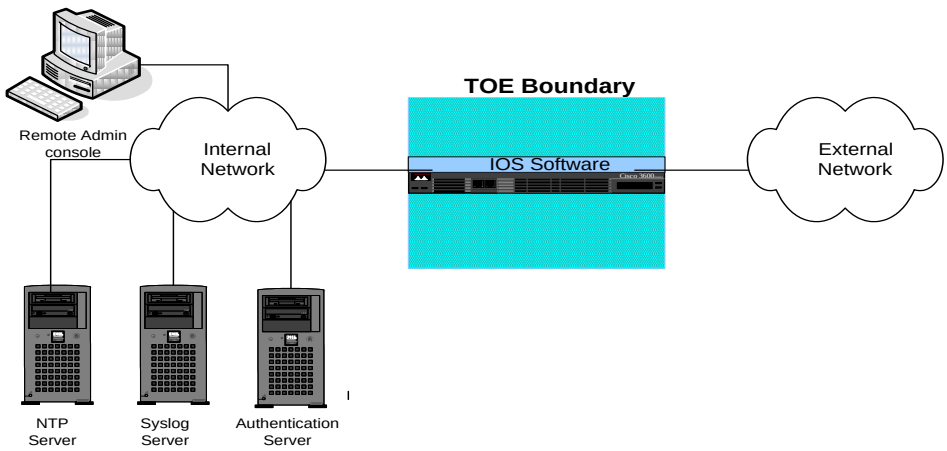
TOE	• One or more RSP720 Management Cards per chassis (Two Sup cards in one chassis provide Supervisor failover within the chassis.) • Each RSP720 running IOS 15.1(3)S3 (FIPS validated) • RSP720 cards installed into one or more 7613, 7609-S, 7606-S, 7604 or 7603-S (Two chassis can be configured together to support HA with VSS.)Each chassis with one VPN IPSec SPA (ws-ipsec-3) Line Card • With one or more compatible line cards. See Annex B of the ST for the list of compatible cards.

The TOE can optionally connect to an NTP server on its internal network for time services. A syslog server can also be 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.

If the TOE is to be remotely administered, SSHv2 must be used for that purpose. All administrative capabilities can be performed either remotely via SSHv2 or locally using the console port. Both methods access the same Command Line Interface (CLI) functionality.

The TOE can optionally support any line card or service module that is compatible with the supervisors and chassis models included in the TOE (See Annex B of the Security Target). These line cards and service modules are not security-relevant to the CC-evaluated security functional requirements.

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



5.4 Physical Scope of the TOE

The TOE is a hardware and software solution that uses a combination of chassis, supervisor engine, IPSec Card, and line cards: the Cisco 7600 Series Routers (7613, 7609-S, 7606-S, 7604 and 7603-S) with Supervisor RSP720 (RSP720-3CXL-10GE, RSP720-3C-10GE, RSP720-3CXL-GE or RSP720-3C-GE), with Cisco IOS 15.1(3)S3 running on the Supervisor Engine, VPN IPSec SPA (ws-ipsec-3) line card, and any line cards listed in Annex B of the Security Target.

6 Documentation

The following documentation was used as evidence for the evaluation of the Cisco 7600 Series Routers.

6.1 Design Documentation

1. *Cisco 7600 Series Routers Security Architecture Document DRAFT,* Revision 0.2, July 19, 2012
2. *Cisco 7600 Series Routers Functional Specification*, Revision 0.3, September 24, 2012
3. *Cisco 7600 Series Routers TOE Design Specification,* Revision 0.2, July 19, 2012
4. *Annex A: Security Relevant CLI Commands,* March 2, 2012
5. *Annex B: RFC Security Parameter Relevancy*, July 19, 2012

6.2 Guidance Documentation

1. *Cisco 7600 Series Routers Common Criteria Operational User Guidance and Preparative Procedures,* Version 0.5, September 28, 2012

Table 4 - Additional Guidance Documentation

Title	Link
Cisco 7600 Series Router Installation Guide, May 31, 2011	http://www.cisco.com/en/US/docs/routers/7600/Hardware/Chassis_Installation/7600_Series_Router_Installation_Guide/pref.html
Configuration Fundamentals Configuration Guide Cisco IOS Release 15.1S	http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/configuration/15-1s/cf-15-1s-book.html
Authentication, Authorization and Accounting Configuration Guide (Cisco IOS Release 15.1S) in Securing User Services Configuration Guide Library, Cisco IOS Release 15.1S	http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/15-1s/secuser-15-1s-library.html
Network Management Configuration Guide Library, Cisco IOS Release 15.1S	http://www.cisco.com/en/US/docs/ios-xml/ios/net_mgmt/config_library/15-1s/netmgmt-15-1s-library.html
Cisco IOS Security Command Reference	http://www.cisco.com/en/US/products/ps11746/prod_command_reference_list.html
Loading and Managing System Images Configuration Guide, Cisco IOS Release 15.1S	http://www.cisco.com/en/US/docs/ios-xml/ios/sys-image-mgmt/configuration/15-1s/sysimgmgmt-15-1s-book.html
Cisco 7606-S and 7609-S Routers with Supervisor SUP720-3B FIPS 140-2 Non-proprietary Security Policy	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm See #1621
Security Configuration Guide: Zone-Based Policy Firewall Cisco, IOS Release 15.1S	http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/15-1s/sec-data-zbf-15-1s-book.html

Title	Link
IPv6 Configuration Guide, Cisco IOS Release 15.1S	http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-1s/ipv6-15-1s-book.html

6.3 Life Cycle

1. *Configuration Management, Lifecycle and Delivery Procedures for Cisco 7600 Series IOS 15.1(3)S3,* September 2012, Version 1.2

6.4 Testing

1. *7600s EAL2 non-NDPP Project Common Criteria Detailed Test Plan,* Revision 8, 09/25/2012
2. 7600-EAL2-non-NDPP-TestCaseMapping-20120925.xls *Detailed Testing Report for Common Criteria Testing on 7600,* 06/23/2012.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the *Evaluation Team Test Report for the Cisco 7600 Series Routers*, Version 1.0, 28 September 2012. All testing of the product was performed manually.

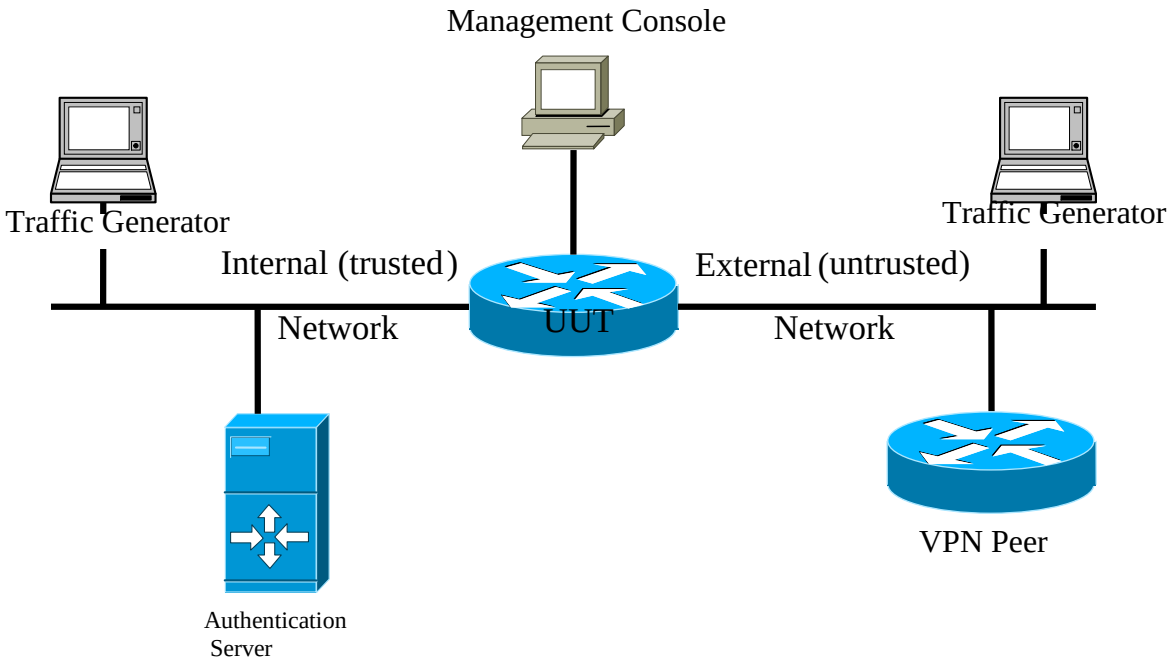
7.1 Developer Testing

At EAL2, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing addressed each of the security functions identified in the ST and interfaces in the design. These security functions include:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Secure management
- Protection of the TSF
- TOE access

7.2 Evaluation Team Independent Testing

The evaluation team installed the product according the *Cisco 7600 Series Routers Common Criteria Operational User Guidance and Preparative Procedures*. With the TOE in the evaluated configuration, the team ran a subset of the vendor test suite and verified the results. The team developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality. The following diagram illustrates the test environment.



The evaluation team testing focused on testing boundary conditions not tested by Cisco. The TOE supports optional use of NTP, syslog, and authentication (RADIUS and TACACS+) servers provided in the operational environment. Cisco test cases demonstrate use of a NTP server to set clock for timestamps, use of a syslog server to export audit records, and use of RADIUS and TACACS+ servers for authentication. Evaluation team tests demonstrated configuration of the TOE to use a RADIUS server but otherwise did not exercise optional servers in the operational environment. For vulnerability testing the evaluation team performed port and vulnerability scanning as well as other team developed tests.

Cisco's test coverage analysis identified 40 security configuration commands for the 7600 Series Routers. Of these commands, 13 are not applicable to the TOE (that is, the commands apply to product features that are not included in the evaluated configuration). The test coverage analysis maped all 27 security relevant TOE commands to Cisco tests. Some of the tests contain steps to verify that unprivileged users cannot execute commands requiring privilege.

The evaluation team repeated a subset of Cisco's tests. The test subset demonstrated 24 of the 27 security relevant TOE commands. The team included tests demonstrating privilege restriction in the test subset. Only three security relevant TOE commands were not covered during team testing: `tacacs-server host`, `tacacs-server key`, and `ntp`. While the `tacacs-server host` and `tacacs-server key` commands were not tested by the evaluation team, the evaluation team did demonstrate the corresponding commands for a RADIUS server (that is, `radius-server host` and `radius-server key`).
.

8 Evaluated Configuration

The Target of Evaluation (TOE) is a hardware configuration in Cisco 7600 Series of routers running IOS 15.1(3)S3 software. The evaluate hardware configurations consist of:

- One or more 7600 series chassis (7613, 7609-S, 7606-S, 7604 or 7603-S),
- One or more RSP720 Management Cards per chassis,
- One or more compatible line cards as identified in the Security Target.
- One VPN IPSec SPA (ws-ipsec-3) Line Card per Chassis

To use the product in the evaluated configuration, the product must be configured as specified in the *Cisco 7600 Series Routers Common Criteria Operational User Guidance and Preparative Procedures* document.

.

9 Results of the Evaluation

Science Applications International Corporation (SAIC) determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 augmented with ALC_FLR.2 and ALC_DVS.1. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation and validation efforts were finished on December 4, 2012.

10 Validator Comments

The validation team's observations support the evaluation team's conclusion that Cisco 7600 Series Routers meet the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- The user of this product should carefully review the restrictions on the evaluated configuration documented in the Clarification of Scope Section 4.2 of this report.
- If audit records are to be protected from loss, the administrator must follow the administrator guidance for management and maintenance of audit logs to move them to secure archival storage. The protection of these archival records is beyond the scope of the evaluated configuration.
- Cisco IOS does not provide process separation.
- ARP poisoning of dynamic routing tables remains possible, so Cisco recommends configuring static tables to prevent ARP poisoning on the ESR 7600.
- Use of the GUI to manage the 7600 was not evaluated. Only the CLI interface should be used for management.
- The TOE provides VPN services in the evaluated configuration. However, only some aspects of VPN were subject to evaluation. Specifically, only IPsec features of the TOE were evaluated. (See FCS_IPSEC_EXT.1 in the ST).
- The 7600 Router series supports many interface line cards and add-on modules. However, only line cards listed in the ST Annex B: Compatible Cisco 7600 Series Line Cards are part of the evaluated configuration. No add-on modules were included in the evaluation.

11 Security Target

The Security Target is identified *Cisco 7600 Series Routers Security Target*, Revision 0.13, dated November 27, 2012.

.

12 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

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

- Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R3, July 2009.
- Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R3, July 2009.
- Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R3, July 2009.
- Common Criteria Project Sponsoring Organisations. *Common Methodology for Information Technology Security Evaluation*, Version 3.1 R3, July 2009.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 2.0, September 8, 2008.
- *Cisco 7600 Series Routers Security Target*, Revision 0.13, November 27, 2012.
- Science Applications International Corporation. *Evaluation Technical Report for the Cisco 7600 Series Routers Part 1 (non-Proprietary)*, Version 1.0, 28 September 2012.
- Science Applications International Corporation. *Evaluation Technical Report for the Cisco 7600 Series Routers Part 2 (Proprietary)*, Version 2.0, 28 September 2012.
- *Evaluation Team Test Report for Cisco 7600 Series Routers (SAIC and Cisco Proprietary)*, Version 1.0, September 28, 2012