National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Cisco Embedded Services Router 5900 Series, Integrated Services Router 800 Series, Integrated Services Router 800M Series & Industrial Router 800 Series, Version 1.0

Report Number: CCEVS-VR-VID10666-2015

Dated: December 22, 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

Jean Petty

Chris Thorpe

Stelios Melachrinoudis

The MITRE Corporation

Common Criteria Testing Laboratory

Pascal Patin

Anthony Busciglio

Dereck Oshin

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) 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 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 5 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 Embedded Services Router 5900 Series, Integrated Services Router 800 Series, Integrated Services Router 800M Series & Industrial Router 800 Series Target of Evaluation (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 was completed by Acumen Security in December 2015. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) with Errata #3 and Network Device Protection Profile Extended Package VPN Gateway (VPNGWEP).

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) with Errata #3 and Network Device Protection Profile Extended Package VPN Gateway (VPNGWEP). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, 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.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Compliance 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(s) to which the product is conformant.
- 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
TOE	Cisco Embedded Services Router 5900 Series (ESR 5900), Integrated Services Router 800 Series (ISR-800), Integrated Services Router 800M Series (ISR-800M) & Industrial Router 800 Series (IR-800)
Protection Profile	U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) with Errata #3 and Network Device Protection Profile Extended Package VPN Gateway (VPNGWEP)
Security Target	Cisco Embedded Services Router 5900 Series (ESR 5900), Integrated Services Router 800 Series (ISR-800), Integrated Services Router 800M Series (ISR-800M) & Industrial Router 800 Series (IR-800) Security Target
Evaluation Technical Report	VID 10666 Common Criteria NDPP Assurance Activity Report, version 1.0
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria	Acumen Security

Testing Lab (CCTL)	Montgomery Village, MD
CCEVS Validators	Jean Petty, Chris Thorpe, Stelios Melachrinoudis

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target. The subsections below provide an overview of the Cisco ESR 5900, ISR-800 Series, ISR-800M Series and IR-800 Series Target of Evaluation (TOE).

3.1 ESR 5900

The TOE is comprised of both software and hardware. The hardware is comprised of the Cisco 5915 and 5940 Embedded Services Router. The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release 15.5(3)M.

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

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

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

The important features of the Cisco ESR 5900 include the following –

- Onboard hardware encryption for security protocols like IPsec, AES and IKE.
- Five 10/100 Fast Ethernet ports (two routed and three switched) supporting autonegotiation
- One RS-232 console port supporting modem flow-control signaling

3.2 ISR-800 -

The TOE is comprised of both software and hardware. The hardware is comprised of the following models: C887VAG-4G-GA-K9, C892FSP-K9, C897VA-K9, C897VAG-LTE-GA-K9, C899G-LTE-GA-K9 and C899G-LTE-NA-K9. The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release 15.5(3)M.

The important features of the Cisco ISR-800 include the following –

- Secure broadband and Metro Ethernet access with concurrent services for enterprise small branch offices.
- Redundant WAN links: Fast Ethernet (FE), V.92, ISDN Basic, Rate Interface (BRI), Gigabit Ethernet (GE), ADSL2+/VDSL (Annex A/B/M), Multimode G.SHDSL, and Small Form-Factor Pluggable (SFP)
- Site-to-site remote-access and VPN services: IP Security (IPsec) VPNs
- 1000BASE-T Gigabit Ethernet WAN port
- 10/100BASE-T Fast Ethernet WAN port on the Cisco 891 or 1-port Gigabit Ethernet WAN port
- 1-port Gigabit Ethernet SFP socket for WAN connectivity
- Dedicated console and auxiliary ports for configuration and management

3.3 ISR 800M

The TOE is comprised of both software and hardware. The hardware is comprised of the Cisco C841M-4X and the Cisco C841M-8X. The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release 15.5(3)M.

Some of the most important features of the ISR-800M include –

- Best suited for secure WAN connectivity for very small locations, transactional data from ATM machines and kiosks, locations with limited WAN services requiring serial connectivity.
- Integrate a Gigabit Ethernet switch and redundant Gigabit Ethernet WAN uplinks
- VPN Support - Integrated IPsec, Group Encrypted Transport, Cisco Dynamic Multipoint VPN (DMVPN), Cisco FlexVPN, Cisco EasyVPN.
- Public-key-infrastructure (PKI) support.
- Semimodular architecture that supports pluggable Cisco WAN Interface Modules (WIMs)

3.4 IR 800

The TOE is comprised of both software and hardware. The hardware is comprised of the Cisco 829GW-LTE-NA-AK9 IR, Cisco 829GW-LTE-VZ-AK9 IR, Cisco 829GW-LTE-GA-EK9 IR, Cisco 829GW-LTE-GA-ZK9 IR, Cisco 809G-LTE-VZ-K9 IR, Cisco 809G-LTE-GA-K9 IR and Cisco 809G-LTE-NA-K9 IR. The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release 15.5(3)M.

Some of the important features of the IR-800 include –

- Ruggedized fixed form factor router that targets mobile/vehicle applications and includes Wi-Fi to provide connectivity in non-carpeted IT spaces, Industrials, Utilities, Transportation, Infrastructure, Industrial M2M application, asset monitoring, Smart Grid, and Utility Application.
- Flash memory and main memory are factory default and cannot be upgraded by end user.
- The flash memory contains the Cisco IOS software image and the boot flash contains the ROMMON boot code

- 4-port GE LAN Switch, 1 GE RJ45 copper WAN or WAN/LAN module

Cisco IOS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.6 Logical Scope of the TOE.

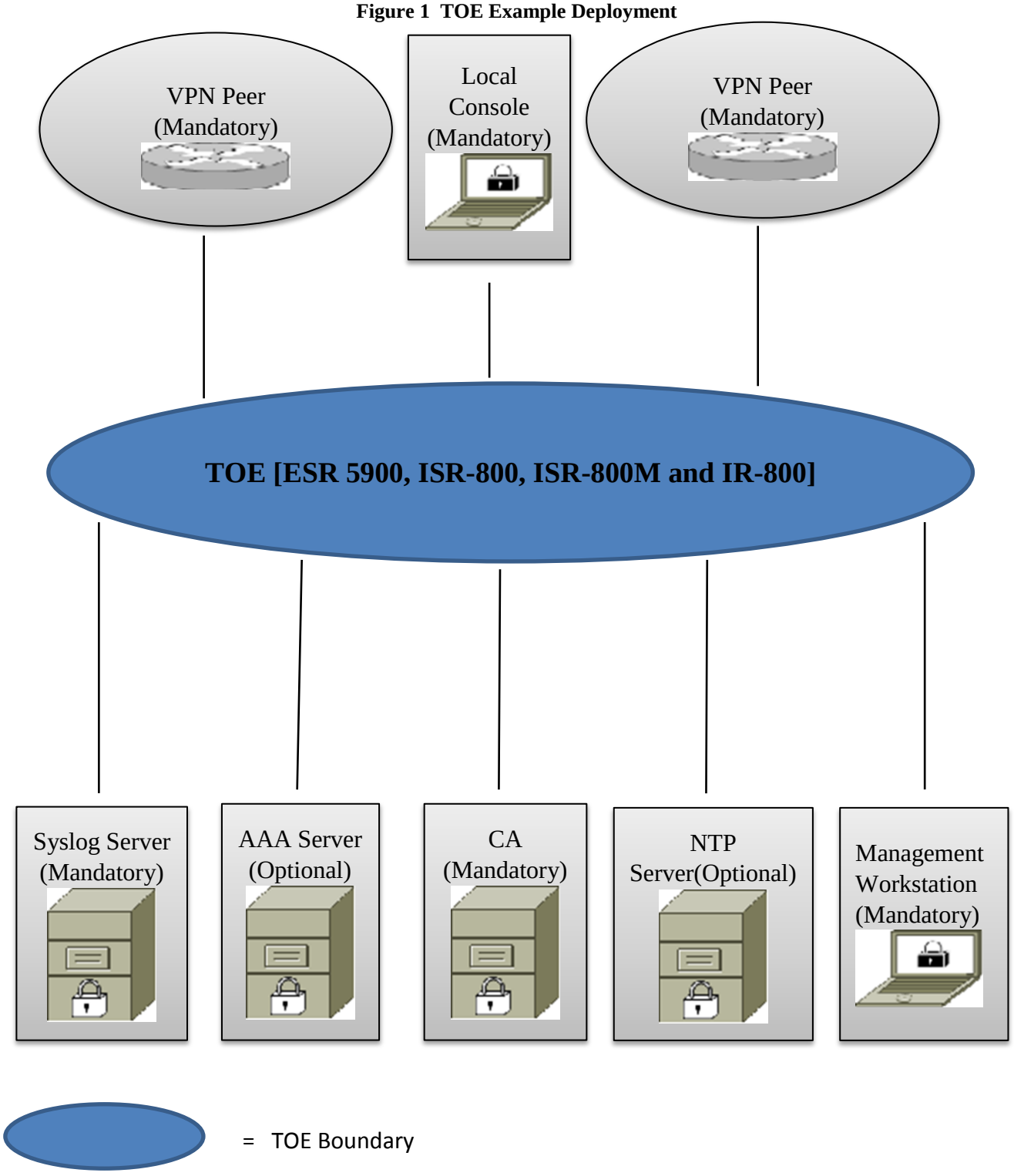
3.5 Example TOE Deployment

All of the routers included in the TOE implement the security functions the same way and implement the same set of security functions and SFRs; the difference between the different models is related to performance and/or other non-security relevant factors.

Figure 1, below, provides a visual depiction of an example TOE deployment. The figure includes the following:

- TOE, i.e., any of the models listed in the TOE Evaluated Configuration.
- The following are considered to be in the IT Environment:
    - (2) VPN Peers
    - Management Workstation
    - Authentication Server
    - NTP Server
    - Syslog Server
    - Local Console
    - CA

Figure 1 TOE Example Deployment



4 Security Policy

The TOE is comprised of several security features, as identified below.

- Security Audit
- Cryptography Support
- User Data Protection
- Identification & Authentication
- Security Management
- Packet Filtering
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

In addition, the TOE implements all RFCs of the NDPP as necessary to satisfy testing/assurance measures prescribed therein. The security features of the TOE are described in more detail in the subsections below.

4.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE 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.

4.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. This cryptography is described in more detail in the ST. Refer to the ST for specific certificate information.

4.3 User 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.

4.4 Identification and Authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The TOE supports use of IKEv1 (ISAKMP) and IKEv2 pre-shared keys for authentication of IPsec tunnels. 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.

4.5 Security Management

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

- Administration of the TOE locally and remotely;
- 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 verification of the updates;
- Configuration of IPsec functionality;
- 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. Management of the TSF data is restricted to Security Administrators. The ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE is restricted to authenticated administrators.

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

4.6 Packet Filtering

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

4.7 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords.

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

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 unauthorized software.

Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads.

4.8 TOE Access

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

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

4.9 Trusted Path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2, and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers. The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server, as well as to protect communications with a CA or remote administrative console.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumption	Assumption Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
A.NO_GENERAL_PURPOSE	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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
Reproduced from U.S. Government Approved Protection Profile - Network Device Protection Profile (NDPP) Extended Package VPN Gateway Version 1.1	
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threat	Threat Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.

Threat	Threat Definition
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	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.
T.UNAUTHORIZED_ACCESS	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.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.
Reproduced from the VPNGWEP	
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T. NETWORK_ACCESS	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.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies.
T.TSF_FAILURE	Security mechanisms of the TOE mail fail1, leading to a compromise of the TSF.

[1] Should read – "may fail" and not "mail fail". Typo in the PP.

Threat	Threat Definition
T.REPLAY_ATTACK	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.
T.DATA_INTEGRITY	A malicious party attempts to change the data being sent – resulting in loss of integrity.

5.3 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) with Errata #3 and Network Device Protection Profile Extended Package VPN Gateway (VPNGWEP).
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco Embedded Services Router 5900 Series (ESR 5900), Integrated Services Router 800 Series (ISR-800), Integrated Services Router 800M Series (ISR-800M) & Industrial Router 800 Series (IR-800) Security Target [ST], version 1.0;
- Cisco Embedded Services Router 5900 Series (ESR 5900), Integrated Services Router 800 Series (ISR-800), Integrated Services Router 800M Series (ISR-800M) & Industrial Router 800 Series (IR-800) Security Target Operational User Guidance and Preparative Procedures [AGD], version 1.0;

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE consists of one or more physical devices as specified in below and includes the Cisco IOS software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS 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. BGP, EIGRP, EIGRPv6 for IPv6 OSPF, OSPFv3 for IPv6, PIM, and RIPv2 routing protocols are used on all of the ISR models.

The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the ISR 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. The TOE can leverage the services provided by this RADIUS AAA server to provide single-use authentication to administrators. A CA server is used to provide the TOE with a valid certificate during certificate enrollment. 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.

The TOE is a hardware and software solution that makes up the router models as follows:

- Cisco 5915 ESR
- Cisco 5940 ESR
- C887VAG-4G-GA-K9
- C892FSP-K9
- C897VA-K9
- C897VAG-LTE-GA-K9
- C899G-LTE-GA-K9
- C899G-LTE-NA-K9
- Cisco C841M-4X
- Cisco C841M-8X
- Cisco 829GW-LTE-NA-AK9 IR
- Cisco 829GW-LTE-VZ-AK9 IR
- Cisco 829GW-LTE-GA-EK9 IR
- Cisco 829GW-LTE-GA-ZK9 IR
- Cisco 809G-LTE-VZ-K9 IR
- Cisco 809G-LTE-GA-K9 IR
- Cisco 809G-LTE-NA-K9 IR

The network on which they reside is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco ESR

5900, ISR-800, ISR-800M and IR-800 Series Common Criteria Operational User Guidance and Preparative Procedures document and are downloadable from the http://cisco.com web site.

7.2 Excluded Functionality

The following functionality is excluded from the evaluation.

Excluded Functionality	Exclusion Rationale
Non-CC mode of operation on the	This mode of operation includes non-allowed operations.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) with Errata #3 and Network Device Protection Profile Extended Package VPN Gateway (VPNGWEP).

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for the Cisco Embedded Services Router 5900 Series (ESR 5900), Integrated Services Router 800 Series (ISR-800), Integrated Services Router 800M Series (ISR-800M) & Industrial Router 800 Series (IR-800), which is not publically available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDPP with VPNGWPP. The Independent Testing activity is documented in the Assurance Activities Report, which is publically available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Embedded Services Router 5900 Series (ESR 5900), Integrated Services Router 800 Series (ISR-800), Integrated Services Router 800M Series (ISR-800M) & Industrial Router 800 Series (IR-800) that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the NDPP with VPNGWPP.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the

evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the NDPP, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

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

10 Validator Comments & Recommendations

The validators suggest that the consumer pay special attention to the evaluated configuration of the device(s) 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

Cisco Embedded Services Router 5900 Series (ESR 5900), Integrated Services Router 800 Series (ISR-800), Integrated Services Router 800M Series (ISR-800M) & Industrial Router 800 Series (IR-800) Security Target [ST], version 1.0.

13 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.

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 and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.