AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2002/24

Cisco Systems Inc.

Cisco IOS/IPSec

Issue 1.0
September 2002

Issued by:

Defence Signals Directorate - Australalasian Certification Authority

AISEP

AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

EAL4

This is to certify that

Cisco IOS/IPSec,
On IOS versions 12.2(6) and 12.1(10)E

in the category of

Network Security

produced by

Cisco Systems Inc.

has been evaluated under the terms of the
Australasian Information
Security Evaluation Program
and complies with the requirements for
Common Criteria
Evaluation Assurance Level 4

....
Australasian Certification Authority   Date: 19 September 2002

Certificate number: 2002/24

Common Criteria

Executive Summary

This report describes the findings of the evaluation of Cisco IOS/IPSec, developed by Cisco Systems Inc., to the Common Criteria (CC) Evaluation Assurance Level EAL4. The report concludes that the product has met the target assurance level of CC EAL4, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product. The evaluation was performed by CSC Australia and was completed on 2 August 2002.

Cisco IOS/IPSec is the implementation of the IPSec standard within the IOS operating system installed in Cisco Systems routers. IPSec provides confidentiality, authenticity and integrity for IP data transmitted between trusted networks over untrusted links or networks. The scope of the evaluation is limited to the components of the IOS software image that implement the IPSec function and functions that are relevant to the secure configuration and operation of IPSec, as well as the optional hardware acceleration modules that may be installed in the relevant routers to process the cryptographic functions. The scope of the evaluation is described in detail in Chapter 3: Intended Environment for the TOE. Details of the specific IOS images, supporting routers and hardware modules that have been considered in this evaluation can be found in Chapter 7: Evaluated Configuration.

Cisco IOS/IPSec has been found to uphold the claims made in the Security Target (ref [10]), and potential customers are urged to consult this document before planning to implement the product. In particular, Cisco IOS/IPSec has been found to provide the claimed confidentiality, authenticity and integrity for IP data traffic, when configured according to an organisational security policy that identifies which connected networks are trusted, which packet flows are to be protected by the IPSec functions and which remote IPSec enabled routers are associated with each secure channel. The security services provided by Cisco IOS/IPSec have been found, when implemented in the intended environment, to be resistant to attackers that may attempt to gain access to the router and compromise its security functions by altering its configuration and to attackers that may attempt to compromise the data within protected channels. Details of the requirements for the organisational security policy can be found in Chapter 2: Security Policy, and details of the assumptions that have been made in defining the intended operational environment for Cisco IOS/IPSec can be found in Chapter 3: Intended Environment for the TOE.

Ultimately, it is the responsibility of the user to ensure that Cisco IOS/IPSec meets their requirements. For this reason, it is ***strongly*** recommended that prospective users of the product obtain a copy of the Security Target (ref [10]) from the product vendor, and read this Certification Report thoroughly prior to deciding whether to purchase or implement the product.

Table of Contents

Executive Summary ii
Table of Contents iii
Chapter 1 Introduction 1
Intended Audience 1
Identification 1
Description of the TOE 1
Chapter 2 Security Policy 3
Organisational Security Policy 3
TOE Security Policies 3
Chapter 3 Intended Environment for the TOE 5
Secure Usage Assumptions 5
Clarification of Scope 5
Chapter 4 TOE Architecture 8
Chapter 5 Documentation 10
Chapter 6 IT Product Testing 11
Functional Testing 11
Penetration Testing 12
TOE Configuration for Testing 12
Chapter 7 Evaluated Configuration 15
Procedures for Determining the Evaluated Version of the TOE 18
Chapter 8 Results of the Evaluation 20
Evaluation Procedures 20
Certification Result 20
Common Criteria EAL4 20
General Observations 20
Chapter 9 Recommendations 21
Scope of the Certificate 21
Installation and Configuration Guide 21
TOE Administration 21
Security Policy 21
Log Management 22
Denial of Service 22
Malformed SNMP Message-Handling Vulnerability 22
Cryptography 23
Appendix A Security Target Information 25
Security Objectives for the TOE 25
Security Objectives for the Environment 25
Threats 26
Summary of the TOE Security Functional Requirements 26
Security Requirements for the IT Environment 27
Security Requirements for the Non-IT Environment 27
Appendix B Acronyms 28
Appendix C References 29

Chapter 1 Introduction

Intended Audience

This certification report states the outcome of the IT security evaluation of Cisco IOS/IPSec. It is intended to assist potential users when judging the suitability of the product for their particular requirements, and to provide advice to security administrators to ensure that the product is used in a secure manner.

This report should be read in conjunction with the Security Target for Cisco IOS/IPSec (ref [10]), which provides a full description of the security requirements and specifications that were used as the basis of the evaluation. A copy of the Security Target can be obtained from Cisco Systems.

Identification

Table 1 provides identification details for the evaluation. For details of the router platforms and associated optional hardware acceleration modules included in the evaluated configuration refer to Chapter 7: Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Cisco IOS/IPSec
Software Version	IOS Release 12.2(6) and 12.1(10)E
Security Target	Security Target for Cisco IOS/IPSec, Version 3.7, 30 July 2002
Protection Profile Claims	The Security Target does not claim conformance to any PPs
Evaluation Level	CC EAL 4
Conformance Result	CC Part 2 Extended CC Part 3 Conformant
Evaluation Technical Report	Evaluation Technical Report for Cisco IOS/IPSec, Version 2.0, 2 August 2002
Version of CC	CC Version 2.1, August 1999
Version of CEM	CEM-99/045 Version 1.0, August 1999
Sponsor	Cisco Systems Australia
Developer	Cisco Systems Inc.
Evaluation Facility	CSC Australia
Certifiers	Kirk Cheney, Chris Pennisi, Doug Stuart, Lachlan Turner

Description of the TOE

The Target of Evaluation (TOE) is the implementation of the IPSec standard within Cisco routers. The TOE is called Cisco IOS/IPSec.

Cisco routers run an embedded operating system called IOS (Internetworking Operating System), which is a proprietary operating system kernel written by Cisco Systems. Cisco's IOS supports a wide range of internetworking functions and capabilities, and operates on a number of Cisco platforms.

The Cisco IPSec implementation is a software function included in IOS. The cryptographic processing required for IPSec can be performed either in software, or using an optional hardware acceleration module that can be plugged into the router platform. The TOE comprises Cisco's implementation of IPSec in IOS release 12.2(6) and 12.1(10)E on various router platforms, including optional hardware acceleration.

The TOE provides confidentiality, authenticity and integrity for IP data transmitted between Cisco Systems routers. A common application of this functionality is the construction of Virtual Private Networks (VPNs).

The TOE only addresses:

- The IPSec function, and
- Functions relevant to the secure configuration and operation of the IPSec function.

Other IOS functions that do not support IPSec are not included in this evaluation.

For further information on the specific hardware platforms and IOS images included in the evaluated configuration refer to Chapter 7: Evaluated Configuration, or Section 1.2 of the Security Target (ref [10]).

Chapter 2 Security Policy

This section outlines the security policies or rules that the TOE must enforce, or comply with, for correct operation.

Organisational Security Policy

The TOE is designed to enforce the Organisational Security Policy (OSP), which must be defined by the owners of the TOE. The OSP, P.Connectivity, requires that the TOE owners must:

- specify whether networks connected to the TOE are trusted or untrusted;
- define which packet flows are to be protected by the TOE; and
- associate each protected packet flow with a peer TOE that will decrypt/encrypt the flow.

It should be noted that IPSec functionality can only be invoked in a situation in which at least one interface of the router is connected to a trusted network, at least one other interface is connected (directly, or indirectly) to an untrusted network, and at least one remote router is recognised, and configured, as an IPSec peer node. This is because IPSec is a standard used to create secure channels, and a secure channel is only meaningful if the endpoints are trusted and the network between the endpoints is not. This is why each of the elements identified in this OSP is essential for the correct operation of the TOE.

The requirements for P.Connectivity are defined in Section 3.3, Organisational Security Policies, of the Security Target (ref [10]).

TOE Security Policies

The TOE Security Policies (TSPs) define the security policies that the TOE must comply with in order to enforce the organisational security policy and the security functional requirements. The Security Target (ref [10]) contains a single explicit security policy for the TOE, which is the Information Flow Control SFP. The Information Flow Control policy defines the behaviour of the TOE in handling the packet flows to be protected, as defined in the organisational security policy, and can be summarised as:

- **Information Flow Control TSP**: The TOE is to be configured to provide protection including authentication, integrity and confidentiality based on the following attributes:
    - Receiving/transmitting interface
    - Source/destination IP address
    - Source/destination TCP port number
    - Other IPSec attributes (including within the ESP packet header)

In addition, the security policy model provided by the developers defines a number of implied TSPs, drawn from the collection of security functional requirements. These can be summarised as:

- **Management Session TSP**: The TOE shall maintain two administrative roles: privileged users and unprivileged users. Remote users shall be permitted to access the TOE based on network parameters as applied to an access list and defined in the organisation security policy (P.Connectivity). Users local to the TOE console will be authenticated before privileged access is granted. Both remote and local users are to be authenticated before administrative access to the TOE is granted;

- **System Message Management TSP**: The TOE is to provide logging of system messages. Only privileged users are to be permitted to view the system message log or to modify the log configuration. Any changes to the system message configuration are to be logged within the message log currently in use;

- **Time Management TSP**: The TOE is to maintain a reliable time source to enable the time stamping of audit log messages and enforce time-reliant key management functions. Only an authenticated privileged user may be permitted to configure the time functions of the TOE.

Chapter 3 Intended Environment for the TOE

This section outlines the requirements and assumptions that govern the intended environment in which the TOE is designed to operate, and for which the TOE has been evaluated, and clarifies the scope of the evaluation. Organisations wishing to implement the TOE in its evaluated configuration should review the evaluation scope to confirm that all the required functionality has been included in the evaluation, and must ensure that any assumed conditions are met in their operational environment.

Secure Usage Assumptions

The evaluation of the Cisco IOS/IPSec product took into account the following assumptions about the secure usage of the TOE:

- Administrators are assumed to be non-hostile and trusted to perform their duties correctly;

- Administrators of the TOE are assumed to have been trained to enable them to securely configure the TOE;

- The router containing the TOE is assumed to be located in a physically secure environment, preventing an attacker from gaining physical access to that router;

- If the TOE is configured to use digital certificates, the issuing Certificate Authority (CA) is trusted or evaluated to at least the same level as the TOE; and

- Clock sources external to the scope of the TOE are placed in a secure location, and configured accurately so as to provide a trusted clock source for the TOE's internal clock. This includes hardware clocks within the TOE casing or Network Time Protocol (NTP) servers located on a trusted network.

Clarification of Scope

The scope of the evaluation is limited to those claims made in the Security Target (ref [10]). All security related claims in the Security Target were evaluated by CSC Australia as a component of the evaluation. A summary of the Security Target is provided in Appendix A of this Certification Report.

The TOE is the implementation of the IPSec standard within specific versions of the IOS operating system, installed on specific router platforms, and includes the optional hardware accelerators. The evaluated configurations for the TOE are given in Chapter 7: Evaluated Configuration.

The evaluation covered the IPSec function and supporting functions that enable secure configuration and operation of the IPSec function. The TOE provides the following (evaluated) security functionality:

- **IPSec Internet Key Exchange (IKE):** IKE authenticates IPSec peers using pre-shared keys, RSA keys or digital certificates. It also handles the exchange of session keys and negotiates the parameters used during IPSec Encapsulating Security Payload (ESP);

- **IPSec Encapsulating Security Payload (ESP):** ESP provides confidentiality, integrity, and authenticity for packet flows when added to an IP packet. Confidentiality is implemented using the DES and 3DES ciphers, integrity and authenticity are implemented using digital signatures based on the MD5 and SHA-1 standards. ESP also provides replay detection;

- **Cryptographic Maps:** Cryptographic Maps are used by the TOE to specify the packet flow to be protected, the IPSec options and the parameters to be used while performing encryption, the means of identifying the peer TOE that will decrypt the packet flow and the interfaces of the TOE-enabled router that will be enabled to establish the secure channel;

- **Packet Filtering:** The TOE performs input packet filtering by applying an access control list to specific interfaces of the TOE-enabled router. The access control list can include IP protocol, source/destination IP address and source/destination UDP/TCP port number. Packets not matching the access list are logged and discarded by the router;

- **System Messages:** The TOE generates system diagnostic messages to identify specific TOE operations. The resulting messages can be directed to the system console, SYSLOG server or a logging buffer internal to the TOE;

- **Management Interfaces:** The TOE can be configured, managed and operated from a direct local console connection or an in-band network connection. The network connection can take the form of a Telnet session for interactive command line (CLI) operation, TFTP file transfer protocol or SNMP management software for read-only device monitoring. Interactive CLI sessions (console or telnet) require authentication before access to the security configuration interface is granted;

- **Management of Time:** The TOE maintains real time using a reliable software clock that interfaces to either an internal hardware clock or a Network Time Protocol (NTP) server; and

- **Key Management:** The TOE generates public/private keys for use with a Public Key Infrastructure (PKI). The TOE interacts with a certificate authority using the Simple Certificate Enrolment Protocol (SCEP) to download a certificate authority's digital certificate and to request and download a digital certificate for the TOE itself.

The hardware accelerator modules that are included in the TOE are listed below, noting the appropriate router platforms:

- MOD1700-VPN
  - Cisco 1720 and 1750
- AIM-VPN/BP
  - Cisco 2610, 2611, 2612, 2613, 2620 and 2621
- NM-VPN/HP
  - Cisco 3620 and 3640
- AIM-VPN/HP
  - Cisco 3660
- SM-ISM, SA-ISA, SM-VAM or SA-VAM
  - Cisco 7120 and 7140
- SA-ISA or SA-VAM
  - Cisco 7204 and 7206

Potential users of the TOE are advised that the following **have not been evaluated** as part of the evaluation of Cisco IOS/IPSec:

- IOS security functions not included in the IPSec security standard, including: IOS firewall functionality, Intrusion Detection System, and RADIUS and TACACS+ authentication mechanisms;
- IOS functions not relevant to the secure configuration and operation of the IPSec implementation;
- The IPSec Application Header (AH) protocol, an alternative to the ESP protocol, which is also supported by Cisco routers;
- The IPSec Transport mode, an alternative to the Tunnel mode, which is also supported by Cisco routers;
- Router hardware and firmware, with the exception of the hardware accelerator modules listed above; and
- The use of RSA public/private key pairs (RSA nonces) on platforms with a VPN Accelerator Module (VAM) installed.

Chapter 4 TOE Architecture

The TOE functionality is implemented entirely in software, as part of either IOS version 12.2(6) or version 12.1(10)E, as appropriate, with the exception of the cryptographic processes, which are implemented on the appropriate hardware accelerator, if it is installed. The optional hardware accelerators are included as part of the TOE. There is no reliance by the TOE on any other components of the host router's hardware, software or firmware for providing security functions.

The developer's high level design identifies a number of functional subsystems of the TOE, which each implement a component of the security functionality. They are described here:

- **Access Control Lists (ACL):** The ACL subsystem permits or denies traffic flows through the TOE based on the TSP. Additionally, the ACL subsystem controls management access to the TOE by accepting only sessions from previously configured management stations according to the organisation security policy (P.Connectivity);

- **Clock:** The clock subsystem maintains the real-time clock function of the TOE. The clock subsystem acquires time information from a time source that is external to the TOE, either the host router's internal hardware clock or a Network Time Protocol (NTP) server located on a trusted network;

- **Command Line Interface (CLI):** The CLI provides an interactive interface to allow the configuration and monitoring of TOE security functions either via a local console connection or ACL permitted remote management stations;

- **Crypto Engine:** The crypto engine subsystem provides cryptographic services to other subsystems within the TOE. The functions of the subsystem are implemented in software, however, a hardware accelerator module will be utilised if installed on the router platform. Services provided include:
    - Cryptographic encapsulation/decapsulation;
    - Encryption/decryption (using DES and 3DES algorithms);
    - Message authentication/validation (using the SHA-1 and MD-5 algorithms);
    - Diffie-Hellman processing;
    - Digital signature generation and verification; and
    - Generation and validation of anti-replay tags;

- **IPSec:** The IPSec subsystem provides the mechanism for the establishment of a secure communications channel between trusted networks and the transmission and receipt of traffic flows over that channel. The traffic flows travelling via the secure channel can have confidentiality, authenticity and integrity assured by utilising IPSec ESP functions;

- **IPSec Internet Key Exchange (IKE):** The IKE subsystem is utilised to provide authentication and subsequent negotiation of a security association (SA) between two IPSec peers over an untrusted network. IKE can authenticate IPSec peers using pre-shared keys, RSA nonces or digital signatures generated by a certificate authority (CA);

- **Logger:** The logger subsystem receives system messages from other subsystems within the TOE and stores the messages in an internal buffer or external logging system according to configuration;

- **PKI:** The purpose of the PKI subsystem is to authenticate the TOE with IPSec peers using digital certificates when such authentication is specified by the TSP. If required, the PKI subsystem will communicate with a certificate authority (CA) to authenticate other IPSec peers; and

- **User Authentication:** The user authentication subsystem is used to authenticate administrative users before they are allowed access to the privileged functions of the TOE via the interactive CLI interface.

Chapter 5 Documentation

It is important that Cisco IOS/IPSec is used in accordance with the guidance documentation in order to ensure the secure usage of the TOE. The developer provides the following documents with the product:

- Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS/IPSec (ref [12]); and
- Cisco Product Documentation (Disks 1 and 2) (ref [13]).

The Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS/IPSec guide is intended to provide administrators with the information that they need to enable them to install and configure the TOE in a manner that is consistent with the evaluated configuration.

The Cisco Product Documentation CD-ROM disks contain the full documentation for the Cisco IOS operating system, and is intended to provide administrators with additional information to assist them with configuring and maintaining the TOE. Disk 1 contains the installation software for the Cisco documentation interface, including a web-browser, and Disk 2 contains the documentation files. It should be noted that the evaluated version of the documentation was the October 2001 release, which is the version that will be distributed with the TOE. The CD-ROMs are updated monthly, and the information is also available online or in printed paper form. If administrators wish to use more recent documentation, they should be aware that the relevant guidance may have been updated and they may no longer be adhering to the evaluated configuration.

There are no components of Cisco IOS IPSec that are accessible to non-administrative users, so there is no requirement for additional user-level guidance documentation.

Chapter 6 IT Product Testing

The objectives associated with the testing phase of evaluation can be placed into the following categories:

- **Functional testing:** Tests performed to ensure that the TOE operates according to its specification and is able to meet the requirements stated in the Security Target (ref [10]).
- **Penetration testing:** Tests conducted to identify exploitable vulnerabilities in the TOE's intended operational environment.

Functional Testing

In this phase the evaluators analysed evidence of the developer's testing effort, including test coverage and depth analyses, test plans and procedures, and expected and actual results, to gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE. In addition, the evaluators drew on this evidence to develop a set of independent tests, comprising a sample of the developer tests, in order to verify that the test results matched those recorded by the developers, as well as a selection of independent functional tests that expanded on the testing done by the developers.

The developer's functional testing was conducted using specialised regression testing facilities housed within the development site, using automated scripts. The evaluators repeated approximately 60% of these automated test procedures using the developer's test facilities, a sample that was considered sufficient to establish confidence in the accuracy of the automated testing process. The tests were chosen to test the core functionality of the TOE, and can be traced back to the core TOE Security Functions. The results of these evaluator tests were consistent with the actual results recorded by the developers from their own testing.

In addition, the evaluators conducted additional functional tests in their own laboratory using routers supplied by the developer. The test configuration is described in the TOE Configuration for Testing section, below.

The evaluators developed and executed a test plan to independently verify that the attributes of the Cisco IOS/IPSec implementation behaved as defined throughout the evaluation. The evaluators tested the following:

- Identification and Authentication
- Generation of Keys and Certificates
- Internet Key Exchange
- Management of Time
- Management Interfaces
- System Messages
- Packet Filtering
- IPSec ESP

The functions tested covered the full range of Security Functional Requirements identified in the Security Target (ref [10]), with the exception of those that rely on cryptographic operations. Whilst the tests devised did ensure that the cryptography was being implemented, testing of the actual cryptographic processes is considered the responsibility of the national cryptographic authority. In Australia, the cryptographic functions have been evaluated by the Defence Signals Directorate, as the national authority, and found suitable for Australian and New Zealand Government use. Australian and New Zealand Government users should carefully read the Cryptography section in Chapter 9: Recommendations.

Penetration Testing

The developers performed a vulnerability analysis of the Cisco IOS/IPSec, in order to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the TOE. This analysis included a search for possible vulnerability sources in the evaluation deliverables, the intended TOE environment, public domain sources and internal Cisco sources. A number of potential vulnerabilities relevant to the product type were identified and in each case the developers were able to show that the vulnerability was not exploitable on the TOE version of the product in the intended environment.

Based on the information given in the developer’s vulnerability analysis, the evaluators were able to devise a penetration test plan that would test that the TOE is resistant to penetration attacks performed by an attacker with low to medium attack potential, exploiting any of the identified vulnerabilities. In addition, the evaluators performed an independent vulnerability analysis in order to identify any possible vulnerabilities that had not been addressed by the developers. Based on this information, the evaluators identified further independent penetration tests. All penetration tests were conducted concurrently using the test facilities set up at the evaluators’ laboratory, testing all platforms as described in the TOE Configuration for Testing section, below.

Upon completion of the penetration testing activity, the evaluators concluded that the TOE did not display any susceptibility to vulnerabilities obtained from the developer or those from the evaluators’ independent vulnerability analysis.

TOE Configuration for Testing

The full range of hardware platforms and IOS images with which the TOE is compliant is shown in Chapter 7: Evaluated Configuration, and in the Security Target (ref [10]). For the purposes of testing, a sample of these platforms was chosen, as it was determined that each family of routers use the same family of IOS images. Therefore, each router family was represented in the testing subset rather than each supported router. All supported hardware acceleration modules were included in the test set. The evaluators conducted independent testing on the hardware platforms indicated in Table 2 below:

Table 2: Router test configurations

Model	Optional IPSec Hardware acceleration Module	IOS Release
1720	None	12.2(6)
	MOD1700-VPN	
1750	None	12.2(6)
	MOD1700-VPN	
2621	None	12.2(6)
	AIM-VPN/BP	
3620	None	12.2(6)
	NM-VPN/MP	
3640	None	12.2(6)
	NM-VPN/MP	
3660	None	12.2(6)
	AIM-VPN/HP	
7140	None	12.2(6)
	SM-ISM	
	SA-ISA	
7206	None	12.2(6)
	SA-ISA	
7140	None	12.1(10)E
	SM-ISM	
	SA-ISA	
7206	None	12.1(10)E
	SA-VAM	

Similarly, since each IOS image file was sourced from a common source code tree, it was determined that the image file that supported the most features for each family should be used for testing, as all feature sets contained in all other images would also be present in this image file. It should be noted, however, that although other features were present in the image, such as firewall or IDS functionality, these features were not part of the TOE, and therefore not tested. Table 3 identifies those IOS images that were used during the testing phase for those platforms with the 12.2(6) version of the IOS code. Table 4 identifies those IOS images used in the testing phase for the 12.1(10)E version of the TOE.

Table 3: IOS version 12.2(6) image files used for testing

Cisco 7200 with 12.2(6)	
c7200-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS IPSEC 3DES
Cisco 7100 with 12.2(6)	
c7100-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
Cisco 3660 with 12.2(6)	
c3660-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
Cisco 3640 with 12.2(6)	
c3640-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
Cisco 3620 with 12.2(6)	
c3620-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
Cisco 2610, 2611, 2612, 2613, 2620, 2621 with 12.2(6)	
C2600-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
Cisco 1750 with 12.2(6)	
c1700-bk9no3r2sv3y-mz.122-6.bin	IP/IPX/AT/IBM/VO/FW/IDS PLUS IPSEC 3DES
Cisco 1720 with 12.2(6)	
c1700-bk9no3r2sy-mz.122-6.bin	IP/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES

Table 4: IOS version 12.1(10)E image files used for testing

Cisco 7200 with 12.1(10)E	
c7200-jk2o3s-mz.121-10.E.bin	ENTERPRISE/FW/IDS IPSEC 3DES
Cisco 7100 with 12.1(10)E	
c7100-jk2o3s-mz.121-10.E.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES

Chapter 7 Evaluated Configuration

The TOE encompasses two versions of the IOS software: 12.2(6) and 12.1(10)E. The evaluated configuration includes various hardware platforms with optional IPSec hardware acceleration modules. The Cisco Systems router platforms and modules included in the evaluated configuration are identified in Table 5 below.

Table 5: Cisco products that support Cisco IOS/IPSec

Model Family	Models	Optional IPSec Hardware Acceleration Module	IOS Release
1700	1720, 1750	MOD1700-VPN	12.2(6)
2600	2610, 2611, 2612, 2613, 2620, 2621	AIM-VPN/BP	12.2(6)
3600	3620, 3640	NM-VPN/MP	12.2(6)
	3660	AIM-VPN/HP	12.2(6)
7100	7120,7140	SM-ISM or SA-ISA	12.2(6)
		SM-VAM or SA-VAM	12.1(10)E
7200	7204, 7206	SA-ISA	12.2(6)
		SA-VAM	12.1(10)E

There are a number of IOS images with different IOS feature sets also included in the evaluated configuration. These images are identified in Table 6 below.

Table 6: IOS images included in the evaluated configuration

IOS Image Name	IOS Feature Set
Cisco 7200 with 12.2(6)	
c7200-a3jk8s-mz.122-6.bin	ENTERPRISE/SNASW IPSEC 56
c7200-dk8o3s-mz.122-6.bin	DESKTOP/IBM/FW/IDS IPSEC 56
c7200-dk8s-mz.122-6.bin	DESKTOP/IBM IPSEC 56
c7200-ik8o3s-mz.122-6.bin	IP/FW/IDS IPSEC 56
c7200-ik8s-mz.122-6.bin	IP IPSEC 56
c7200-jk8o3s-mz.122-6.bin	ENTERPRISE/FW/IDS IPSEC 56
c7200-jk8s-mz.122-6.bin	ENTERPRISE IPSEC 56
c7200-a3jk9s-mz.122-6.bin	ENTERPRISE/SNASW IPSEC 3DES
c7200-dk9o3s-mz.122-6.bin	DESKTOP/IBM/FW/IDS IPSEC 3DES
c7200-ik9o3s-mz.122-6.bin	IP/FW/IDS IPSEC 3DES
c7200-ik9s-mz.122-6.bin	IP PLUS IPSEC 3DES
c7200-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS IPSEC 3DES
c7200-jk9s-mz.122-6.bin	ENTERPRISE IPSEC 3DES

Cisco 7100 with 12.2(6)	
c7100-ik8o3s-mz.122-6.bin	IP/FW/IDS IPSEC 56
c7100-ik8s-mz.122-6.bin	IP IPSEC 56
c7100-jk8o3s-mz.122-6.bin	ENTERPRISE/FW/IDS IPSEC 56
c7100-jk8s-mz.122-6.bin	ENTERPRISE IPSEC 56
c7100-ik9o3s-mz.122-6.bin	IP/FW/IDS IPSEC 3DES
c7100-ik9s-mz.122-6.bin	IP PLUS IPSEC 3DES
c7100-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
c7100-jk9s-mz.122-6.bin	ENTERPRISE IPSEC 3DES
Cisco 3660 with 12.2(6)	
c3660-a3jk8s-mz.122-6.bin	ENTERPRISE/SNASW PLUS IPSEC 56
c3660-ik8o3s-mz.122-6.bin	IP/FW/IDS PLUS IPSEC 56
c3660-ik8s-mz.122-6.bin	IP PLUS IPSEC 56
c3660-jk8o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 56
c3660-jk8s-mz.122-6.bin	ENTERPRISE PLUS IPSEC 56
c3660-a3jk9s-mz.122-6.bin	ENTERPRISE/SNASW PLUS IPSEC 3DES
c3660-ik9o3s-mz.122-6.bin	IP/FW/IDS PLUS IPSEC 3DES
c3660-ik9s-mz.122-6.bin	IP PLUS IPSEC 3DES
c3660-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
c3660-jk9s-mz.122-6.bin	ENTERPRISE PLUS IPSEC 3DES
c3660-telcoentk9-mz.122-6.bin	TELCO PLUS FEATURE SET IPSEC 3DES
Cisco 3640 with 12.2(6)	
c3640-a3jk8s-mz.122-6.bin	ENTERPRISE/SNASW PLUS IPSEC 56
c3640-ik8o3s-mz.122-6.bin	IP/FW/IDS PLUS IPSEC 56
c3640-ik8s-mz.122-6.bin	IP PLUS IPSEC 56
c3640-jk8o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 56
c3640-jk8s-mz.122-6.bin	ENTERPRISE PLUS IPSEC 56
c3640-a3jk9s-mz.122-6.bin	ENTERPRISE/SNASW PLUS IPSEC 3DES
c3640-ik9o3s-mz.122-6.bin	IP/FW/IDS PLUS IPSEC 3DES
c3640-ik9s-mz.122-6.bin	IP PLUS IPSEC 3DES
c3640-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
c3640-jk9s-mz.122-6.bin	ENTERPRISE PLUS IPSEC 3DES
Cisco 3620 with 12.2(6)	
c3620-a3jk8s-mz.122-6.bin	ENTERPRISE/SNASW PLUS IPSEC 56
c3620-ik8o3s-mz.122-6.bin	IP/FW/IDS PLUS IPSEC 56
c3620-ik8s-mz.122-6.bin	IP PLUS IPSEC 56
c3620-jk8o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 56

c3620-jk8s-mz.122-6.bin	ENTERPRISE PLUS IPSEC 56
c3620-a3jk9s-mz.122-6.bin	ENTERPRISE/SNASW PLUS IPSEC 3DES
c3620-ik9o3s-mz.122-6.bin	IP/FW/IDS PLUS IPSEC 3DES
c3620-ik9s-mz.122-6.bin	IP PLUS IPSEC 3DES
c3620-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
c3620-jk9s-mz.122-6.bin	ENTERPRISE PLUS IPSEC 3DES
Cisco 2610, 2611, 2612, 2613, 2620, 2621 with 12.2(6)	
c2600-a3jk8s-mz.122-6.bin	ENTERPRISE/SNASW PLUS IPSEC 56
c2600-ik8o3s-mz.122-6.bin	IP/FW/IDS PLUS IPSEC 56
c2600-ik8s-mz.122-6.bin	IP PLUS IPSEC 56
c2600-jk8o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 56
c2600-jk8s-mz.122-6.bin	ENTERPRISE PLUS IPSEC 56
c2600-a3jk9s-mz.122-6.bin	ENTERPRISE/SNASW PLUS IPSEC 3DES
c2600-ik9o3s-mz.122-6.bin	IP/FW/IDS PLUS IPSEC 3DES
c2600-ik9s-mz.122-6.bin	IP PLUS IPSEC 3DES
c2600-jk9o3s-mz.122-6.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
c2600-jk9s-mz.122-6.bin	ENTERPRISE PLUS IPSEC 3DES
Cisco 1750 with 12.2(6)	
c1700-bk8no3r2sv3y-mz.122-6.bin	IP/IPX/AT/IBM/VOICE/FW/IDS PLUS IPSEC 56
c1700-k8o3sv3y-mz.122-6.bin	IP/VOICE/FW/IDS PLUS IPSEC 56
c1700-k8sv3y-mz.122-6.bin	IP/VOICE PLUS IPSEC 56
c1700-bk9no3r2sv3y-mz.122-6.bin	IP/IPX/AT/IBM/VO/FW/IDS PLUS IPSEC 3DES
c1700-k9o3sv3y-mz.122-6.bin	IP/VOICE/FW/IDS PLUS IPSEC 3DES
c1700-k9sv3y-mz.122-6.bin	IP/VOICE PLUS IPSEC 3DES
Cisco 1720 with 12.2(6)	
c1700-bk8no3r2sy-mz.122-6.bin	IP/IPX/AT/IBM/FW/IDS PLUS IPSEC 56
c1700-k8o3sy-mz.122-6.bin	IP/FW/IDS PLUS IPSEC 56
c1700-k8sy-mz.122-6.bin	IP PLUS IPSEC 56
c1700-bk9no3r2sy-mz.122-6.bin	IP/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES
c1700-k9o3sy-mz.122-6.bin	IP/FW/IDS PLUS IPSEC 3DES
c1700-k9sy-mz.122-6.bin	IP PLUS IPSEC 3DES
Cisco 7200 with 12.1(10)E	
c7200-do3s56i-mz.121-10.E.bin	DESKTOP/IBM/FW/IDS IPSEC 56
c7200-ds56i-mz.121-10.E.bin	DESKTOP/IBM IPSEC 56
c7200-io3s56i-mz.121-10.E.bin	IP/FW/IDS IPSEC 56
c7200-is56i-mz.121-10.E.bin	IP IPSEC 56
c7200-jo3s56i-mz.121-10.E.bin	ENTERPRISE/FW/IDS IPSEC 56
c7200-js56i-mz.121-10.E.bin	ENTERPRISE IPSEC 56

c7200-dk2o3s-mz.121-10.E.bin	DESKTOP/IBM/FW/IDS IPSEC 3DES
c7200-ik2o3s-mz.121-10.E.bin	IP/FW/IDS IPSEC 3DES
c7200-ik2s-mz.121-10.E.bin	IP PLUS IPSEC 3DES
c7200-jk2o3s-mz.121-10.E.bin	ENTERPRISE/FW/IDS IPSEC 3DES
c7200-jk2s-mz.121-10.E.bin	ENTERPRISE IPSEC 3DES
Cisco 7100 with 12.1(10)E	
c7100-io3s56i-mz.121-10.E.bin	IP/FW/IDS IPSEC 56
c7100-is56i-mz.121-10.E.bin	IP IPSEC 56
c7100-jo3s56i-mz.121-10.E.bin	ENTERPRISE/FW/IDS IPSEC 56
c7100-js56i-mz.121-10.E.bin	ENTERPRISE IPSEC 56
c7100-ik2o3s-mz.121-10.E.bin	IP/FW/IDS IPSEC 3DES
c7100-ik2s-mz.121-10.E.bin	IP PLUS IPSEC 3DES
c7100-jk2o3s-mz.121-10.E.bin	ENTERPRISE/FW/IDS PLUS IPSEC 3DES
c7100-jk2s-mz.121-10.E.bin	ENTERPRISE IPSEC 3DES

Procedures for Determining the Evaluated Version of the TOE

When placing an order for a Cisco router that is intended to be used with the evaluated IPSec functionality, purchasers should make it clear to their supplier that they wish to receive the evaluated product. They should then receive the correct hardware, software and documentation, including the Installation and Configuration for Common Criteria EAL 4 Evaluated Cisco IOS/IPSec guide (ref [12]), to allow them to configure the product in accordance with the evaluated configuration.

In order for an administrator to determine if a delivered product is consistent with the product that has been evaluated, the procedures identified in the Verification of Image and Hardware IPSec Module section in the Installation and Configuration for Common Criteria EAL 4 Evaluated Cisco IOS/IPSec guide (ref [12]) should be carefully followed. These steps are summarised in the following paragraphs.

The TOE will be delivered to a customer either through a new router purchase with TOE compliant IOS software already loaded, or by upgrading an existing router's IOS software to a TOE compliant version. In addition, the optional hardware acceleration modules may be preinstalled in the router, or may be delivered as a separate item, if it is required.

Upon receipt of a new router or hardware IPSec module, the administrator should verify that the box (packaging) has arrived unopened, that the white tamper-resistant, tamper-evident Cisco Systems bar-coded label on the box is intact, and that the serial numbers on the packing slip match the serial numbers on the actual hardware and the serial numbers on the separately mailed invoice for the equipment. If a discrepancy is identified, contact the equipment supplier (Cisco Systems or an authorised partner).

In order to verify the integrity of an IOS image file, which can be downloaded from the Cisco website, the user must utilise an MD5 hashing program (not provided with the TOE) to generate an MD5 hash of the image file. This checksum is then compared with the MD5 hash for the image, listed in the Installation and Configuration for Common Criteria EAL 4 Evaluated Cisco IOS/IPSec guide (ref [12]), Table 9. If the MD5 hashes do not match, contact Cisco Technical Support.

Once the downloaded IOS image is installed onto the router, the router can be started. Version information can be displayed using the 'show version' command from the prompt, and this version information should be compared to the evaluated versions given in Table 5 above. If a hardware acceleration module has been installed then the output from the 'show version' command will also show the presence of the module. If it does not, or if there is a discrepancy in the software version, contact Cisco Technical Support. If the hardware acceleration module is not installed, or fails to operate, then the router will carry out encryption processes in software.

If the hardware acceleration module is installed and working correctly, the administrator should issue the 'show diag' command. This will return the serial number, version and revision of the hardware module, which should all be checked against the relevant documentation.

Chapter 8 Results of the Evaluation

Evaluation Procedures

The evaluation of Cisco IOS/IPSec was conducted using the Common Criteria for Information Technology Security Evaluation (refs [5] to [8]), under the procedures of the Australasian Information Security Evaluation Program (AISEP) (refs [1] to [4]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (ref [9]) were also upheld during the evaluation and certification of this product.

Certification Result

After due consideration of the Evaluation Technical Report (ref [11]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that Cisco IOS/IPSec upholds the claims made in the Security Target (ref [10]) and has met the requirements of the Common Criteria EAL4 assurance level.

Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability that exploitable vulnerabilities remain undiscovered.

Common Criteria EAL4

EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained through an informal model of the TOE security policy.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

A detailed explanation of the assurance requirements for EAL4 can be found in the Common Criteria, Part 3 (ref [7]).

General Observations

The certifiers would like to acknowledge the invaluable assistance provided by CSC Australia and Cisco Systems staff during the evaluation. The successful completion of this evaluation was made possible by their cooperation, technical assistance and attention to issues raised during the process.

Chapter 9 Recommendations

The following recommendations include information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the certifiers.

Scope of the Certificate

The certificate applies only to versions 12.2(6) and 12.1(10)E of the product on those hardware platforms identified in Table 5 of this report. This certificate is only valid when the Cisco IOS/IPSec product is installed and configured in its evaluated configuration. The evaluated configuration of Cisco IOS/IPSec is described in the Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS/IPSec guide (ref [12]), and in Chapter 7: Evaluated Configuration, and should be verified on receipt of the delivered product.

Cisco IOS/IPSec should only be used in accordance with the intended environment described in Chapter 3: Intended Environment for the TOE, Chapter 3 of the Security Target (ref [10]) and the Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS/IPSec guide (ref [12]).

Importantly, the evaluated configuration does not include the full functionality offered by the Cisco IOS/IPSec product. Potential users of the TOE are advised to consult the Clarification of Scope section, in Chapter 3: Intended Environment for the TOE, for details of which components have been evaluated.

Installation and Configuration Guide

Potential purchasers of the TOE are strongly recommended to obtain a copy of the Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS/IPSec guide (ref [12]) when purchasing the TOE from Cisco. This document contains necessary guidance for an administrator to install and configure the TOE in its evaluated configuration.

TOE Administration

To ensure the competent administration of the TOE, Administrators of the TOE should be trained in Cisco IOS/IPSec administration and have sound knowledge of relevant networking protocols.

Security Policy

As described in Chapter 2: Security Policy, it is essential that the TOE owners define an organisational security policy that identifies the network security requirements for the particular IOS/IPSec implementation. The TOE configuration will determine how packet flows received on one interface will be transmitted on another, and which connections are to be protected by encryption. It is the responsibility of the administrator to ensure that the configuration of the TOE in its intended environment is contributing to the satisfaction of the organisation's network security policy.

Log Management

Administrators should take care in specifying appropriate log management procedures, to prevent the loss of system logs. The TOE can log system messages to the system console, SYSLOG server or an internal logging buffer. If a SYSLOG server is chosen, but configured incorrectly, then system messages will be displayed on the system console. If the logging buffer is chosen the administrator must set the size of the buffer. Once the buffer limit has been exceeded, new system messages will overwrite the older messages. It is important that administrators set the logging options correctly for their environment, and regularly review the system messages.

Denial of Service

Administrators should note that the Security Target for Cisco IOS/IPSec (ref [10]) does not claim the ability to counter any external threats to the availability of the TOE, therefore the TOE has not been evaluated with regards to resistance to denial of service attacks. Attacks which deny the availability of networking devices are common on public networks, and can be extremely difficult to defend against. Whilst the developers have made every effort to counter known vulnerabilities in the IOS operating system which could result in a denial of service to legitimate users, administrators should be aware that vulnerabilities of this nature may still be exploitable in the intended environment for the TOE.

Malformed SNMP Message-Handling Vulnerability

There is a known vulnerability in the way in which some devices handle malformed SNMP messages, which can result in a system crash and reboot, creating a denial of service condition. The evaluated versions of the IOS software are known to be affected by this vulnerability if SNMP management is enabled, which is allowed in the evaluated configuration. Although this vulnerability does not breach any of the security objectives of the TOE, administrators need to be aware that the problem exists.

Cisco have recommended two solutions to reduce the exposure of the TOE to this vulnerability. These are:

- **Turn SNMP off in the TOE:** This is an effective workaround, but removes management capability to the TOE via SNMP;

- **Apply an extended access list (ACL)**: deny protocol UDP, port 161 and 162, at the interface level such that SNMP access to the TOE is allowed only from the network management station.

For further details on this vulnerability, and the configuration commands required to implement these workarounds, administrators should consult the document Cisco Security Advisory: Malformed SNMP Message-Handling Vulnerabilities, available from the Cisco website.

Cryptography

The evaluation of the cryptographic functions of Cisco IOS/IPSec is beyond the scope of the Common Criteria evaluation, and has been undertaken as a separate process by the Defence Signals Directorate, the national cryptographic authority for Australia. Australian and New Zealand Government users wishing to implement the TOE should take the following recommendations into account when planning their operational environment.

The cryptographic functions of Cisco IOS/IPSec have been found to be suitable for Australian Government use, subject to the following recommendations:

- **Key generation:** The Cisco implementation of IPSec allows for manually specifying keys, or automatically generating key material, using ISAKMP and Diffie-Hellman key exchange. For Australian Government use, automatic key generation using ISAKMP should be enabled;

- **Encryption:** Cisco IOS/IPSec supports the DES or 3DES algorithms for encryption. Australian Government users are recommended to use the 3DES algorithm;

- **Authentication:** Cisco IOS/IPSec supports the SHA-1 or MD5 algorithms (both using the HMAC variant) for authentication. Australian Government users are recommended to use the SHA-1 algorithm;

- **IPSec protocol and mode:** The IPSec Transport mode and Application Header (AH) protocol were out of scope, and have not been evaluated. The IPSec Encapsulating Security Payload (ESP) protocol using Tunnel mode should be used, and both encryption and authentication should be enabled;

- **IPSec Security Associations:** Once a Security Association (SA) has been established using IKE, separate keys should be generated for the IPSec exchange (not a refreshed IKE key). Following the expiry of an IPSec SA, new keys should be established. This is done by enabling the Perfect Forward Secrecy (PFS) mode. The SA should be configured to expire regularly, to initiate regeneration. The expiry period should be included in the organisational security policy, and it is suggested that an appropriate period would be in the order of an hour. SA expiry can be achieved through setting the SA lifetime or the SA volume limit. Cisco suggest using the SA volume limit, based on a traffic profile analysis to determine a frequency that is consistent with the security policy. This prevents large numbers of SAs expiring concurrently, generating excessive loads on the network, which may occur when using SA lifetimes on large networks;

- **Router-to-router authentication:** Authentication between routers can be achieved using pre-shared keys, RSA public/private keys or digital certificates. No recommendation is made on which should be used. However, if public key methods are implemented an RSA modulus of at least 1024 bits should be used;

- **Retirement of Routers:** When a router is returned to Cisco for maintenance, or otherwise disposed of, it will be necessary to remove all key material and any configuration information. Australian Government users should contact the Defence Signals Directorate for further information on how to effectively achieve this.

Appendix A Security Target Information

A brief summary of the Security Target (ref [10]) is given below. Potential purchasers should obtain a copy of the full Security Target to ensure that the security enforcing functions meet the requirements of their security policy. A copy of the Security Target can be obtained from Cisco Systems.

Security Objectives for the TOE

Cisco IOS/IPSec has the following IT Security Objectives:

- The TOE must provide the means for ensuring that a packet flow has been received from a trusted source;
- The TOE must protect the confidentiality of packet flows transmitted to/from the TOE over an untrusted network;
- The TOE must ensure that any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected;
- The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt packet flows between instances of the TOE and when kept in short and long-term storage;
- The TOE must provide a means to detect that a packet flow transmitted to the TOE has not been copied by an eavesdropper and retransmitted to the TOE; and
- The TOE must prevent unauthorised changes to its configuration.

Security Objectives for the Environment

Cisco IOS/IPSec has the following IT Security Objectives for the environment:

- Those responsible for the administration of the TOE must provide a policy that specifies:
  - Whether networks connected to the TOE are trusted or untrusted;
  - The packet flows that are to be protected by the TOE; and
  - The peer TOE that will encrypt/decrypt each packet flow.
- Those responsible for the operation of the TOE must ensure that the TOE environment is physically secure, and management and configuration of the security functions of the TOE are:
  - initiated from a management station connected to a trusted network and protected using the security functions of the TOE;

- undertaken by trusted staff trained in the secure operation of the TOE;
- implemented in conjunction with an evaluated or trusted Certificate Authority (CA), if digital certificates are used for TOE authentication; and
- configured to interface only to trusted clock sources.

Threats

The following threats are addressed by Cisco IOS/IPSec:

- An attacker (whether an insider or outsider) may gain access to the TOE and compromise its security functions by altering its configuration; and
- An attacker may attempt to disclose, modify or insert data within packet flows transmitted/received by the TOE over an untrusted network. If such an attack was successful, then the confidentiality, integrity and authenticity of packet flows transmitted/received over an untrusted path would be compromised.

Summary of the TOE Security Functional Requirements

The Cisco IOS/IPSec SFRs are given below. Full description of these SFRs can be found in Section 5.1 of the Security Target (ref [10]).

- Class FAU: Audit
  - Audit Data Generation (FAU_AUD.1 Explicitly stated SFR)
  - Security Audit Review (FAU_SAR.1)
- Class FCO: Communication
  - Enforced Proof of Origin (FCO_NRO.2)
- Class FCS: Cryptographic Support
  - Cryptographic Key Generation (FCS_CKM.1)
  - Cryptographic Key Distribution (FCS_CKM.2)
  - Cryptographic Key Destruction (FCS_CKM.4)
  - Cryptographic Operation (FCS_COP.1)
- Class FDP: User Data Protection
  - Subset Information Flow Control (FDP_IFC.1)
  - Simple Security Attributes (FDP_IFF.1)
  - Basic Data Exchange Confidentiality (FDP_UCT.1)
  - Data Exchange Integrity (FDP_UIT.1)

- Class FIA: Identification and Authentication
  - User Authentication Before any Action (FIA_UAU.2)
  - Multiple Authentication Mechanisms (FIA_UAU.5)
  - User Identification Before any Action (FIA_UID.2)
- Class FMT: Security Management
  - Management of Security Functions Behaviour (FMT_MOF.1)
  - Management of Security Attributes (FMT_MSA.1)
  - Secure Security Attributes (FMT_MSA.2)
  - Static Attribute Initialisation (FMT_MSA.3)
  - Management of TSF Data (FMT_MTD.1)
  - Restrictions on Security Roles (FMT_SMR.2)
  - Assuming Roles (FMT_SMR.3)
- Class FPT: Protection of the TSF
  - Reliable Time Stamps (FPT_STM.1)
  - Abstract Machine Testing (FPT_AMT.1)
  - TSF Testing (FPT_TST.1)
- Class FTA: TOE Access
  - TOE Session Establishment (FTA_TSE.1)
- Class FPT: Trusted path/channels
  - Inter-TSF Trusted Channel (FTP_ITC.1)

Security Requirements for the IT Environment

None included.

Security Requirements for the Non-IT Environment

None included.

Appendix B Acronyms

ACE	AISEP Certificate Extension
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Appendix C References

[1] AISEP Publication No.1- Description of the AISEP
AP 1, Version 2.0, February 2001
Defence Signals Directorate

[2] AISEP Publication No.2 - The Licensing of the AISEFs
AP 2, Version 2.1, February 2001
Defence Signals Directorate

[3] Manual of Computer Security Evaluation Part I - Evaluation Procedures
EM 4, Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[4] Manual of Computer Security Evaluations Part II - Evaluation Tools and Techniques
EM 5, Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[5] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC)
Version 2.1, August 1999, CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC)
Version 2.1, August 1999, CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC)
Version 2.1, August 1999, CCIMB-99-033

[8] Common Methodology for Information Technology Security Evaluation (CEM)
Version 1.0, August 1999, CEM-99/045

[9] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security
May 2000

[10] Cisco IOS/IPSec Security Target
Version 3.7, 30 July 2002
Cisco Systems Inc.

[11] Cisco IOS/IPSec Evaluation Technical Report (ETR)
Issue 2.0, 2 August 2002
CSC Australia
(EVALUATION-IN-CONFIDENCE)

[12] Installation and Configuration for Common Criteria EAL 4 Evaluated Cisco IOS/IPSec
Version 1.0, July 2002
Cisco Systems Inc.

[13] Cisco Product Documentation (Disks 1 and 2)
October 2001
Cisco Systems Inc.