Security Target For Cisco IOS IPSec

March 2007
Version: 1.0

Conventions

The notation, formatting, and conventions used in this Security Target document are consistent with the conventions used in Version 2.3 of the Common Criteria (CC) document. Selected presentation choices are discussed here to aid the Security Target reader. The CC allows several operations to be performed on functional requirements; refinement, selection, assignment and iteration are defined in paragraph 4.4.1.3.4 of Part 1 of the CC [CC1]. Refinements are indicated by **bold text** and ~~strike-through~~. Selections are enclosed in [square brackets]; assignments are enclosed in [square brackets] and underlined. Iterations are numbered in sequence, as appropriate.

Terminology

In the CC document, many terms are defined in Section 2.3 of Part 1. The terms listed in Table 1 The are a subset of those definitions, and are listed here to aid the user of the Security Target.

Table 1 Common Criteria Acronyms and Expansions

Acronym	Expansion Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table 1 Common Criteria Acronyms and Expansions (continued)

Acronym	Expansion Definition
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
TTP	Trusted Third Party

The terminology in Table 2 is specific to the TOE and its environment; these definitions are also provided to aid the user of the Security Target.

Table 2 TOE Definitions

Term	Definition
3DES	Triple DES (Data Encryption Standard)
AES	Advanced Encryption Standard
Assets	Data transmitted over a network
AH	Authentication Header. A security protocol that provides authentication. AH is embedded in the data to be protected (a full datagram).
End System	A client or server system with an IP address
ESP	Encapsulating Security Payload. A security protocol that provides data confidentiality services and optional authentication and replay-detection services. ESP encapsulates the data to be protected.
Extranet	The interconnection of two or more intranets interconnected with an untrusted network using internetworking devices compliant with the TOE to protect packet flows between the intranets.
IOS	Internetwork Operating System. IOS is a Cisco proprietary core software package that is implemented on almost all Cisco routers and switches.
IKE	Internet Key Exchange. Negotiates the security association between two entities and exchanges key material.

Table 2 TOE Definitions (continued)

Term	Definition
Internetworking_Device	A device that interconnects two or more network segments and forwards IP traffic between the end systems connected to the attached network segments; for example, a router or firewall.
Intranet	An organization's internal network, constructed from trusted networks (typically LANs) interconnected with untrusted networks or network segments using internetworking devices.
IPSec	Internet Protocol Security. A set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of network data.
MD5	Message Digest 5. A one-way hash that combines a shared secret and the message (the header and payload) to produce a 128-bit value. The recipient of the message runs the same hash of the message and compares it with the inserted hash value to yield the same result, indicating that nothing in the packet has been changed in transit.
Network	A single network segment or two or more network segments interconnected by internetworking devices.
Network Segment	A single physical segment to which end systems are connected.
Packet Flow	A unicast flow of IP packets identified by some combination of source/destination IP address, source/destination TCP/UDP port number, type of service (TOS) field, and input interface.
Replay Attack	An attempt by an eavesdropper to capture some portion of a transmission and retransmit it at a later time to gain authorized access to the receiver or to spoof the security functions of the receiver.
RSA	A method of public key encryption developed by Rivest, Shamir, and Adelman at the Massachusetts Institute of Technology.
SA	Security Association
SHA-1	Secure Hash Algorithm 1, similar to MD5, but produces a 160-bit hash value. Takes longer to calculate than MD5, but provides less chance of collision.

Table 2 TOE Definitions (continued)

Term	Definition
User	A human that interacts with the TOE to configure and operate the TOE; for example, an administrator. End users (clients) do not interact with the TOE.
VPN	Virtual Private Networking,. The use of encryption to allow network data to traverse securely between two endpoints over an untrusted network.

Table 3 lists abbreviations that are used when referring to Cisco routers.

Table 3 Cisco Router Terms

Term	Definition
AIM	Advanced Interface Module. An internal plug-in hardware accelerator.
E	Ethernet
PA	Port Adapter (a large, high-performance, modular network interface)
VAM	VPN Accelerator Module. A hardware accelerator in port adapter format.
WIC	Wide Area Network (WAN) Interface Card (a small modular network interface for WANs)

Document Organization

Section 1 provides the introductory material for the security target.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by the TOE.

Section 6 presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

Section 7 provides the Protection Profile claims made by this Security Target.

Section 8 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

Section 8 also provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the requirements. A reference section is provided to identify background material.

Section 1: Introduction

1.1 Identification

Title: Security Target for Cisco IOS IPSec Version 1.0

Authors: Cisco Systems, Inc.

Last Updated: October, 2007

CC Version: Common Criteria for Information Technology Security Evaluation, Version 2.3

Keywords: IPSec

1.2 Security Target Overview

The TOE is the implementation of the IPSec security standard within Cisco Systems routers. Routers are used to construct IP networks by interconnecting multiple smaller networks or network segments. IPSec provides confidentiality, authenticity and integrity for IP data transmitted between trusted (private) networks over untrusted (public) links or networks. The TOE therefore 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 is called Cisco IOS IPSec.

Routers are dedicated hardware devices with purpose written software, which perform many networking functions. The TOE only addresses the following:

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

Table 4 lists the Cisco Systems products that are supported by this TOE.

Note Support for RSA public/private key pairs for IKE authentication requires the use of an IPSec hardware acceleration module. Models listed as using “Built In” modules do not support RSA public/private key pairs for IKE authentication.

Table 4 Cisco Systems Products That Are Supported by the TOE

Model Family	Models	IPSec Hardware Acceleration Module	Cisco IOS Release
Cisco 800	871, 876, 877, 878, 851, 851W, 857, 857W	Built In	Cisco IOS Release 12.4(6)T3
Cisco 1800	1841	Optionally with AIM-VPN/BPII-PLUS	Cisco IOS Release 12.4(7)
	1801, 1802, 1803, 1811, 1812	Built In	Cisco IOS Release 12.4(6)T3
Cisco 2800	2801,2811, 2821, 2851	optionally with AIM-VPN/EPII-PLUS	Cisco IOS Release 12.4(7)

Table 4 Cisco Systems Products That Are Supported by the TOE (continued)

Model Family	Models	IPSec Hardware Acceleration Module	Cisco IOS Release
Cisco 3800	3825	optionally with AIM-VPN/EPII-PLUS	Cisco IOS Release 12.4(7)
	3845	optionally with AIM-VPN/HPII-PLUS	Cisco IOS Release 12.4(7)
Cisco 7200	7204, 7206	SA-VAM2+	Cisco IOS Release 12.4(7)
Cisco 7300	7301	SA-VAM2+	Cisco IOS Release 12.4(7)
Cisco 7600 Catalyst 6500	Any 6500/7600 with Supervisor Engine 720, 720-3B, or 720-3BXL	SPA-IPSEC-2G	Cisco IOS Release 12.2(33)SRA

1.3 CC Conformance Claim

This TOE conforms with Part 2 and Part 3 of the CC, version 2.3.

2.0 TOE Description

This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

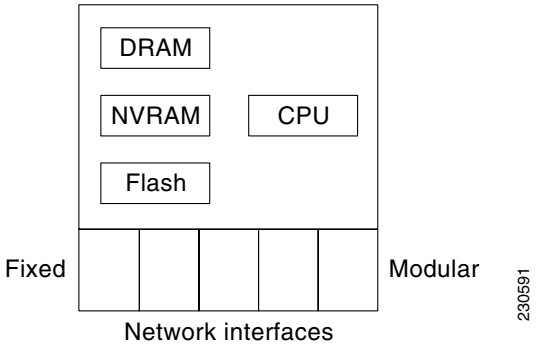
2.1 Product Type

The TOE operates within routers (which are internetworking devices) running the Cisco Internetwork Operating System (IOS).

Routers that support the TOE have a number of common hardware characteristics.

- Central processor that supports all system operations, such as an Intel Pentium, PowerPC, MIPS
- Dynamic memory, used by the central processor for all system operations
- Flash memory, used to store the operating system image
- Non-volatile memory, which stores configuration parameters used to initialize the system at system startup
- Multiple physical network interfaces (minimally two). Some models will have a fixed number and type of interfaces; some models will have slots that accept additional network interfaces.

Figure 1 Common Hardware Components of a Cisco Router



The basic operation of a router is as follows:

1. At system startup, the operating system is transferred from Flash memory to dynamic memory using a built-in hardware bootstrap. (Some models execute the operating systems directly from Flash memory.)
2. The operating system reads the configuration parameters from non-volatile memory, builds the necessary data structures in dynamic memory, and commences operation.
3. IP packets are forwarded to the router over one or more of it's physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the router. This processing typically results in the IP packets being forwarded out of the router over another interface, or dropped in accordance with a configured policy.

2.1.1 Cisco IOS Routers

Routers forward packets from one network segment to another based on network layer information (such as an IP address). Interconnected routers will exchange information to determine the optimal path along which network traffic should be forwarded. The primary function of a router is to provide connectivity between networks of end systems. Routers can also filter packets to permit or deny packet flows.

All Cisco routers use common operating system software called the Internetwork Operating Systems (IOS). For a Cisco router to be compliant with the TOE, it must be equipped with the appropriate version of the Cisco IOS software that includes the IPSec function and configured in accordance with the TOE. The TOE-compliant routers and Cisco IOS software versions are identified in Table 4.

2.2 General TOE Functionality

The primary security function of the TOE is the use of IPSec to provide confidentiality, authenticity, and integrity services for packet flows. Other functions of the TOE support this primary function.

This section describes IPSec options that are supported by the TOE and the TOE functions that support IPSec. A more detailed description of the operation of IPSec can be found in Appendix A.

2.2.1 IPSec

IPSec is a proposed Internet standard developed by the IETF and described in RFCs 2401-2410 and 2451. It provides network data encryption at the IP packet level to guarantee the confidentiality, authenticity, and integrity of IP packets. IPSec only supports IP packets; other network protocols must be encapsulated within IP to be encrypted with IPSec.

Individual IP packets encrypted with IPSec can be detected during transmission, but the IP packet contents (payload) cannot be read. IPSec encrypted packets are forwarded through an IP network in exactly the same manner as normal IP packets, allowing IPSec encrypted packets to be transported across networks and internetworking devices that do not participate in IPSec.

The actual encryption and decryption of IP packets occurs only at devices that are capable of, and configured for, IPSec. When an IP packet is transmitted or received by an IPSec-enabled device, it is encrypted or decrypted only if the packet meets criteria defined by the administrator. These criteria are typically described in the form of access-lists.

Internetworking devices such as routers are used to connect networks together to form larger networks. They are therefore logical places in which to implement IPSec to provide confidentiality, authenticity, and integrity for packet flows passing from one network to another.

This is the functionality described by the TOE; for example, internetworking devices compliant with the TOE are deployed at the edges of untrusted networks (such as the Internet), to provide secure communications between two trusted networks that are physically separated. Cleartext (unencrypted) packet flows that enter an internetworking device from the trusted network side are encrypted by the TOE and forwarded across the untrusted network. When the encrypted packet flow reaches the remote internetworking device, the TOE decrypts the traffic before forwarding it into the remote secure network. IP Packets are encrypted at one internetworking device's outbound interface and decrypted at the other device's inbound interface.

Table 5 lists the IPSec options that are supported by the TOE.

Note Support for RSA public/private key pairs for IKE authentication requires the use of an IPSec hardware acceleration module. Models listed as using "Built In" modules do not support RSA public/private key pairs for IKE authentication.

Table 5 IPSec Options Supported by the TOE

Function	Operation
Authentication between TOEs	IPSec Internet Key Exchange (IKE) with one of the following options: • Pre-shared keys • RSA public/private keys • Digital certificates
Confidentiality of packet flows	IPSec Encapsulating Security Payload (ESP) with one of the following options: • Triple DES (3DES) • AES 3DES or AES can use either IPSec Tunnel or Transport Mode.
Integrity and authenticity of packet flows	IPSec Encapsulating Security Payload (ESP) with HMAC keyed hash algorithm using one of the following options: • SHA-1 • MD-5 SHA-1 or MD-5 can use either IPSec Tunnel or Transport Mode.

2.2.2 Inbound Filtering

To enable a router that is configured with IPSec to be "self defending," the TOE includes the inbound filtering functions of the router operating system. This allows (for example) IP packets that are not IPSec to be ignored by the router, which is particularly important as the TOE will typically operate in a router connected to an untrusted network.

2.2.3 Administration

Since the IPSec function is embedded within the router operating system software, configuration, management and operation of IPSec must be undertaken through the normal IOS administrative interfaces provided by the router (console, Telnet, SNMP, syslog, etc). Therefore, the TOE includes these functions. To ensure that only authorized administrators can gain secure access to these interfaces, the security target specifies that remote management be conducted from a management station connected to a trusted network behind a TOE-enabled router with IPSec connections to the remote routers (see section 2.4). Furthermore, to exclude the possibility that the TOE operation could be modified via SNMP, SNMP is supported only in read-only mode.

2.3 Scope and Boundaries

2.3.1 Logical

The TOE is a software function, with optional hardware acceleration, within Cisco routers. Routers are dedicated hardware devices with purpose written software that perform many networking functions. The TOE only addresses:

- The IPSec function, which provides confidentiality, authenticity, and integrity for selected packet flows transmitted and received by the router.
- Functions relevant to the secure configuration and operation of the IPSec function, such as the use of the management interface and configuration of packet filtering.

IPSec within the TOE is shown in Figure 2. (Note that the IPSec hardware provides no additional functions other than increasing performance of the IPSec function.)

Figure 2 IPSec Within the TOE

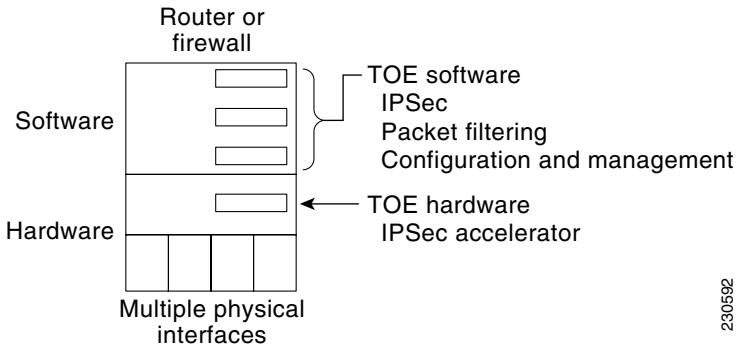
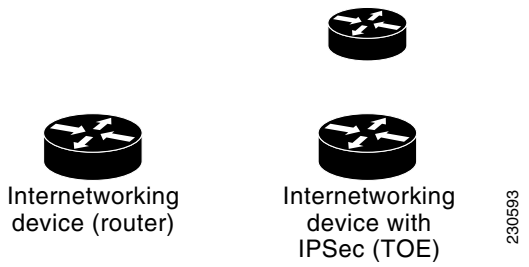


Figure 3 illustrates how the TOE operates as an overlay capability to a standard internetworking device.

Figure 3 TOE Overlay Capability



2.3.2 Physical

The products in which the TOE resides are internetworking devices (routers) and have two or more network interfaces. When the TOE is in use, at least one of the network interfaces of the internetworking device will be attached to a trusted network, and at least one other interface will be attached to an untrusted network. The TOE configuration will determine how packet flows received on one interface

will be transmitted on another. Typically, for packet flows that are to be protected by the TOE security functions, packet flows received on trusted network interfaces will be encrypted using IPSec before being transmitted out an untrusted interface.

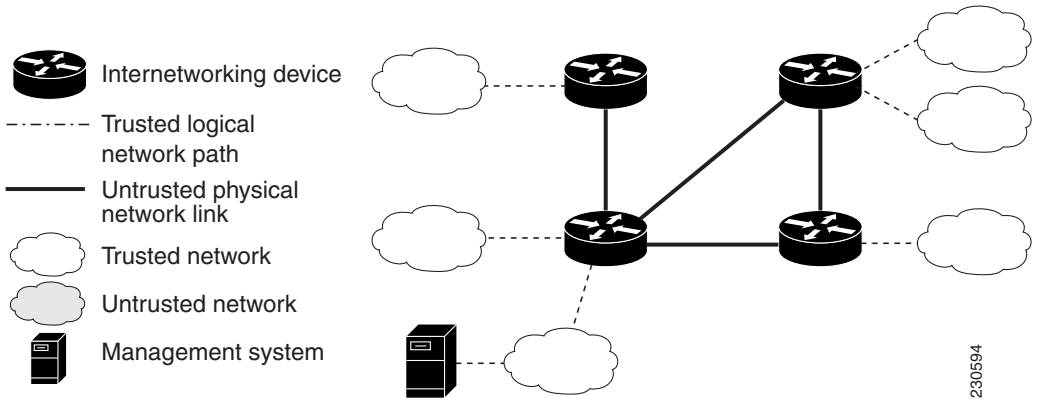
2.4 Application Note

The products defined by the TOE are used to construct secure Intranets and Extranets.

2.4.1 Secure Intranets

Within an Intranet, there can be some network segments that are not trusted because they are physically insecure or outside the control of the owners of the Intranet. Examples of untrusted network segments include wide area links provided by a carrier, microwave links, wireless links, and links shared with other organizations. (See Figure 4)

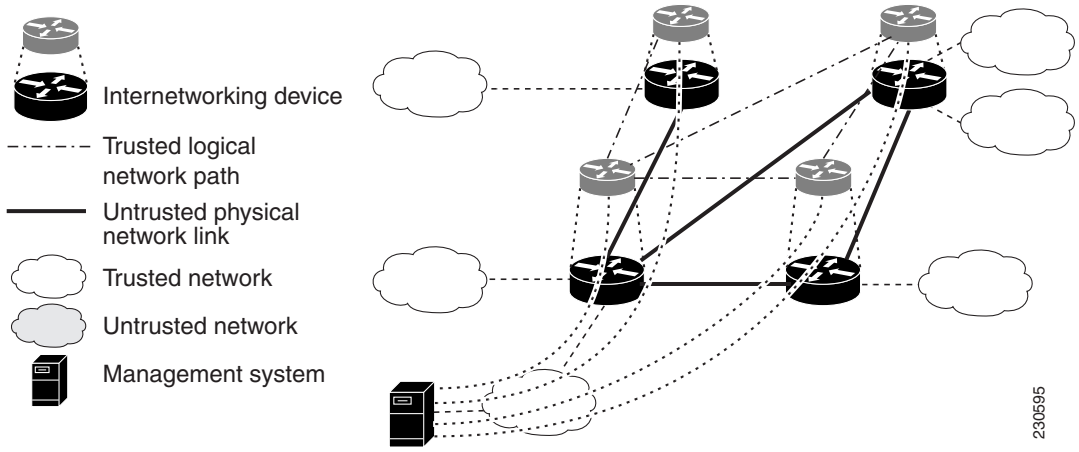
Figure 4 Insecure Intranet



The Intranet may also include transmission paths that cross an insecure network that is not controlled by the owner of the Intranet. A common example is the interconnection of two networks trusted by the same organization over the Internet.

In both cases, the Intranet owner may wish to provide confidentiality, authenticity, and integrity for packet flows transmitted over the untrusted portions of the Intranet. The TOE provides this as a functional extension to existing internetworking devices, thereby, creating a secure Intranet. (See Figure 5)

Figure 5 Secure Intranet

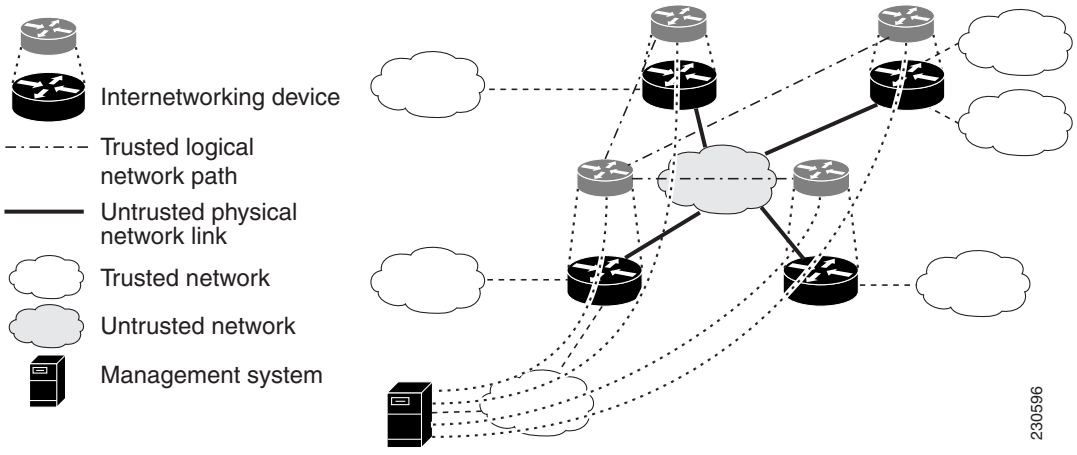


Note The TOE allows the remote internetworking devices to be securely managed and operated by locating the management system on a trusted network. The TOE also uses the confidentiality, authenticity, and integrity security services of the TOE to protect packet flows from the management system to the TOE, in addition to protecting packet flows between trusted network. (See Figure 5)

2.4.2 Extranets

The TOE enables two or more Intranets, interconnected by an untrusted network such as the public Internet, to exchange packet flows in a manner that guarantees the confidentiality, authenticity, and integrity of each packet flow. (See Figure 6)

Figure 6 Secure Extranet



3. TOE Security Environment

To clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and of the manner for which the TOE is intended.
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.

3.1 Secure Usage Assumptions

Table 6 lists assumptions that are made in relation to the operation of TOE.

Table 6 Secure Usage Assumptions

Name	Description
A.NoEvil	As the security functions of the TOE can be compromised by an authorized administrator, administrators are assumed to be non-hostile and trusted to perform their duties correctly.
A.PhySec	As the security functions of the TOE can be compromised by an attacker with physical access to the internetworking device containing the TOE, it is assumed that the internetworking device containing the TOE is located in a physically secure environment.
A.Training	As the security functions of the TOE can be compromised due to errors or omissions in the administration of the security features of the TOE, it is assumed that administrators of the TOE have been trained to enable them to securely configure the TOE.
A.Trusted-CA	When configured to use digital certificates, security functions of the TOE can be comprised if the Certificate Authority (CA) that issued the certificates is not operated in a trusted manner. Thus, it is assumed that the issuing CA is trusted or evaluated to at least the same level as the TOE when the TOE is configured to use digital certificates.
A.SecureTimeSource	Clock sources external to the scope of the TOE should be placed in a secure location and configured accurately 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.

3.2 Threats to Security

The Threat agents against the TOE are attackers with expertise, resources, and motivation that combines to be a low attack potential.

3.2.1 Threats Addressed by the TOE

TOE addresses threats listed in Table 7.

Table 7 Threats Addressed by the TOE

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

3.2.3 Organization Security Policies

Table 8 describes the organizational security policies relevant to the operation of the TOE.

Table 8 Organizational Security Policies

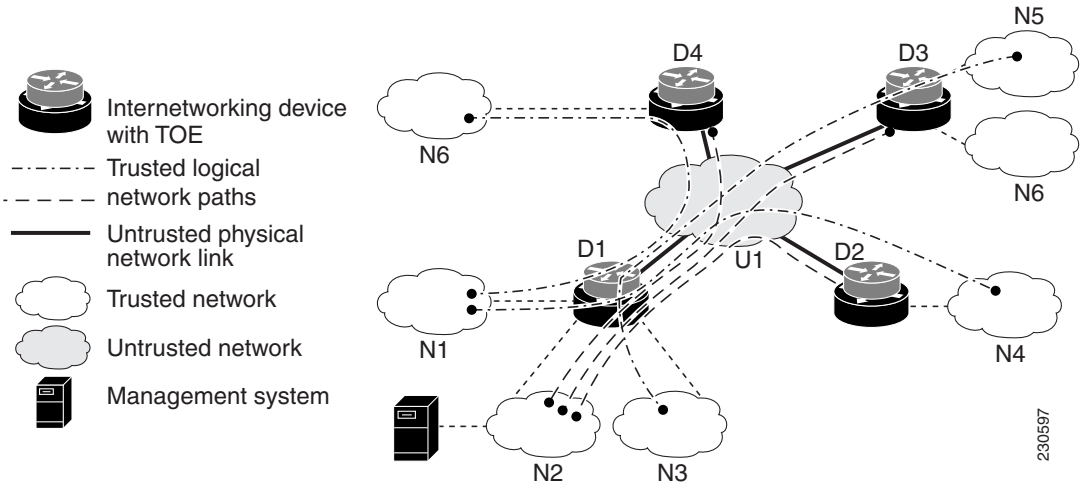
Name	Description
P.Connectivity	The organizational security policy will • Specify whether networks connected to the TOE are trusted or untrusted • Define which packet flows are to be protected by the TOE • Associate each protected packet flow with a peer TOE that will decrypt/encrypt the flow

The organizational security policy, P.Connectivity, is required because it determines how packet flows between trusted networks can be transmitted over an untrusted network. Each instance of the TOE implements a portion of P.Connectivity, which must be matched to, and consistent with, other instances of the TOE for the TOE security functions to be effective.

For example, in Figure 7, an instance of the TOE, D1, has three trusted networks attached to it—N1, N2, N3. It implements a policy highlighted in the table below for three trusted network to network packet flows and three secure management packet flows that cross the untrusted network, U1.

Source	Destination	Peer TOE
N1	N6	D4
N1	N5	D3
N3	N4	D2
N2	D2	D2
N2	D3	D3
N2	D4	D4

Figure 7 Organizational Security Policy



Note In Figure 7, flows are identified solely by the source and destination addresses of IP packets within the flow. As the TOE D1 transmits a packet flow into the untrusted network, it encrypts only the traffic that matches the encryption policy, using an encryption key that has been negotiated with the matching peer. Each peer TOE of D1 must have an implemented matching policy to successfully encrypt and decrypt any flow in accordance with P.Connectivity.

4. Security Objectives

The security objectives are a high-level statement of the intended response to the security problem. These objectives indicate how the security problem, as characterized in the "Security Environment" section of the ST (see the section "3. TOE Security Environment"), is to be addressed.

Table 9 describes security objectives for the TOE, while Table 10 describes objectives for the environment.

4.1 Security Objective for the TOE

Table 9 Security Objectives for the TOE

Name	Description
O.Authenticity	The TOE must provide the means for ensuring that a packet flow has been received from a trusted source.
O.Confidentiality	The TOE must protect the confidentiality of packet flows transmitted to/from the TOE over an untrusted network.
O.Integrity	The TOE must ensure that any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected.
O.Key-Confidentiality	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.
O.NoReplay	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.
O.Secure-Operation	The TOE must prevent unauthorized changes to its configuration.

4.2 Security Objectives for the Environment

Table 10 Security Objectives for the Environment

Name	Description
OE.Policy	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 • The peer TOE that will encrypt/decrypt each packet flow
OE.Secure-Management	Those responsible for the operation of the TOE must ensure that the TOE environment is physically secure, and that management and configuration of the security functions of the TOE are: • Initiated from a management station that is 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 • Configured to interface only to trusted clock sources.

5. IT Security Requirements

5.1 TOE Security Functional Requirements

The TOE functional security requirements are drawn from [CC] Part 2, with the exception of FAU_AUD.1, which is a bespoke security functional component, based on the [CC] Part 2 component FAU_GEN.1.

It was found to be necessary to include FAU_AUD.1 instead of FAU_GEN.1 as the requirements imposed by FAU_GEN.1 are not appropriate for the TOE. The TOE does not record the startup and shutdown of audit functions as the TOE has no facility to shutdown the audit functionality. Additionally, the TOE is designed to remain operational at all times, making the requirement for audit of startup and shutdown redundant.

Selections are enclosed in [square brackets], assignments are enclosed in [square brackets and underlined], refinements are in **bold** and/or ~~strikethrough~~.

5.1.1. Audit data generation (FAU_AUD.1)

The TSF shall be able to generate an audit record of the following auditable events:

a. All auditable events for the [not specified] level of audit; and

b. [Errors during IKE processing,
Errors during IPSEC processing,
When a packet matches a filtering rule, and
Errors during digital certificate processing]

The TSF shall record within each audit record at least the following information:

c. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

d. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other audit relevant information] FAU_AUD.1.2

5.1.2. Audit Review (FAU_SAR.1)

The TSF shall provide [authorized users] with the capability to read [all audit information] from the audit records.FAU_SAR1.1

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.FAU_SAR.1.2

5.1.3. Enforced proof of origin (FCO_NRO.2)

The TSF shall enforce the generation of evidence of origin for transmitted [IP packets protected by the information flow control policy] at all times.[FCO_NRO.2.1]

The TSF shall be able to relate the [IPSec SA peer] of the originator of the information, and the [digital signature] of the information to which the evidence applies.[FCO_NRO.2.2]

The TSF shall provide a capability to verify the evidence of origin of information to [the receiving TOE] given [the successful establishment of an IPSec SA with the transmitting TOE].[FCO_NRO.2.3]

5.1.4. Cryptographic key generation (FCS_CKM.1) (1) RSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [512, 1024 bits] that meet the following: [PKCS #1].[FCS_CKM.1.1]

5.1.5. Cryptographic key generation (FCS_CKM.1) (2) Diffie-Hellman

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Diffie-Hellman key agreement] and specified cryptographic key sizes [56 bit, 168 bit] that meet the following: [PKCS #3].[FCS_CKM.1.1]

5.1.6 - Cryptographic key destruction (FCS_CKM.4)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [no standard].[FCS_CKM.4.1]

5.1.7 - Cryptographic operation (FCS_COP.1(1)) – Encryption

The TSF shall perform [bulk encryption and decryption] in accordance with a specified cryptographic algorithms [3DES, AES] and cryptographic key sizes [168 bit (3DES) and 128, 192, or 256 bit (AES)] that meet the following: [FIPS 46-3, FIPS 197].[FCS_COP.1.1]

5.1.8 - Cryptographic operation (FCS_COP.1(2)) – Signing

The TSF shall perform [digital signing and signature verification] in accordance with a specified cryptographic algorithm [SHA-1, MD5] and cryptographic key sizes [160 bit, 128 bit] that meet the following: [RFC 2404, RFC 2403].[FCS_COP.1.1]

5.1.9 - Subset information flow control (FDP_IFC.1)

The TSF shall enforce the [information flow control SFP] on [

Subject: instances of the TOE

Information: packet flows

Operations: IP packet forwarding, secure remote management].[FDP_IFC.1.1]

5.1.10 - Simple security attributes (FDP_IFF.1)

The TSF shall enforce the [information flow control SFP] based on the following types of subject and information security attributes: [

Subject (TOE instance) Security Attributes

- Policy settings
- TOE identity credentials

Information Security Attributes

- Receiving/transmitting interface;
- Source/destination IP address;
- Source/destination port number;
- IPSec attributes (such as ESP header)].[FDP_IFF.1.1]

The TSF shall permit an information flow between ~~a~~ controlled subjects ~~and~~ of controlled information via a controlled operation if the following rules hold: [if one TOE instance (subject) can authenticate another TOE instance (subject) through the establishment of an IPSec Security Association using the configured policy and identity credentials of the TOE instances]. [FDP_IFF.1.2]

The TSF shall enforce [no additional information flow control SFP rules].[FDP_IFF.1.3]

The TSF shall provide the following [inbound packet filtering] additional capabilities.[FDP_IFF.1.4]

The TSF shall explicitly authorize an information flow based on the following rules: [none].[FDP_IFF.1.5]

The TSF shall explicitly deny an information flow based on the following rules:[the administrator-configured explicit "deny" rules based on the above Information Security Attributes].[FDP_IFF.1.6]

5.1.11 - Basic data exchange confidentiality (FDP_UCT.1)

The TSF shall enforce the [information flow control SFP] to be able to [transmit and receive] objects in a manner protected from unauthorized disclosure.[FDP_UCT.1.1]

5.1.12 - Data exchange integrity (FDP_UIT.1)

The TSF shall enforce the [information flow control SFP] to be able to [transmit and receive] ~~user data~~ packet flows in a manner protected from [modification, insertion and replay] errors.[FDP_UIT.1.1]

The TSF shall be able to determine on receipt of ~~user data~~ a packet flow, whether [modification, insertion and replay] has occurred. [FDP_UIT.1.2]

5.1.13 - User authentication before any action (FIA_UAU.2)

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.[FIA_UAU.2.1]

5.1.14 - Multiple authentication mechanisms (FIA_UAU.5)

The TSF shall provide [password only mechanism; or the combination of username with matching password] to support user authentication.[FIA_UAU.5.1]

The TSF shall authenticate any user's claimed identity according to the [mechanism as defined in the TOE configuration by the privileged administrator]. FIA_UAU.5.2

5.1.15 - User identification before any action (FIA_UID.2)

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.2.1

5.1.16 - Management of security functions behavior (FMT_MOF.1)

The TSF shall restrict the ability to [determine the behavior of, disable, enable, and modify the behavior of] the functions [that implement the information flow control SFP] to [privileged administrators]. FMT_MOF.1.1

5.1.17 - Management of security attributes (FMT_MSA.1)

The TSF shall enforce the [information flow control SFP] to restrict the ability to [

a. query

b. query, modify **and** delete]

the security attributes [TSF configuration] to [

a. administrator

b. privileged administrator.] FMT_MSA.1.1

Application Note: the administrator can only query, whereas the privileged administrator can query modify and delete the TSF configuration.

5.1.18 - Secure security attributes (FMT_MSA.2)

The TSF shall ensure that only secure values are accepted for security attributes.FMT_MSA.2.1

5.1.19 - Static attribute initialization (FMT_MSA.3)

The TSF shall enforce the [information flow control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.FMT_MSA.3.1

The TSF shall allow the [privileged administrator] to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

5.1.20 - Management of TSF data (FMT_MTD.1)

The TSF shall restrict the ability to [

a. query

b. query, modify, delete **and** clear]

the [TSF configuration] to [

a. administrator

b. privileged administrator]. FMT_MTD.1.1

Application Note: the administrator can only query, whereas the privileged administrator can query modify and delete the TSF configuration.

5.1.21Specification of Management Functions (FMT_SMF.1)

The TSF shall be capable of performing the following security management functions: [

a. determine the behavior of, the configuration of functions that implement information flow control SFP;

b. configure the cryptographic TSFs;

c. configure audit management;

d. view all audit information in a manner suitable for interpretation;

e. query, modify and delete the TSF Configuration and its security attributes; and

f. create, delete and modify usernames for use with the access control functions of IOS.

g. configure system time attributes.

]. FMT_SMF.1.1

5.1.22 - Restrictions on security roles (FMT_SMR.2)

The TSF shall maintain the roles: [administrator and privileged administrator]. FMT_SMR.2.1

The TSF shall be able to associate users with roles. FMT_SMR.2.2

The TSF shall ensure that the conditions [that a user has to be authenticated as an administrator before they can be allowed to authenticate as a privileged administrator] are satisfied. FMT_SMR.2.3

5.1.23 - Assuming roles (FMT_SMR.3)

The TSF shall require an explicit request to assume the following roles: [privileged administrator]. FMT_SMR.3.1

5.1.24 - Reliable time stamps (FPT_STM.1)

The TSF shall be able to provide reliable time stamps for its own use. FPT_STM.1.1

5.1.25 - Abstract machine testing (FPT_AMT.1)

The TSF shall run a suite of tests [during initial start-up] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. FPT_AMT.1

5.1.26 - TSF testing (FPT_TST.1)

The TSF shall run a suite of self tests [during initial start-up] to demonstrate the correct operation of [the TSF].[FPT_TST.1.1]

The TSF shall provide authorized users with the capability to verify the integrity of [TSF data]. [FPT_TST.1.2]

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.[FPT_TST.1.3]

5.1.27 - TOE session establishment (FTA_TSE.1)

The TSF shall be able to deny session establishment based on [access control list specifying a combination of source/destination IP address and source/destination TCP/UDP port number].[FTA_TSE.1.1]

5.1.28 - Inter-TSF trusted channel (FTP_ITC.1)

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.[FTP_ITC.1.1]

The TSF shall permit [the TSF] to initiate communication via the trusted channel.[FTP_ITC.1.2]

The TSF shall initiate communication via the trusted channel for [the secure transmission of packet flows between trusted networks, and secure administration and operation of the TOE].[FTP_ITC.1.3]

5.2 TOE Security Assurance Requirements

The TOE meets all the Assurance Requirements prescribed by EAL2 in Part 3 of the CC. The requirements are summarized by Assurance Class in Table 11.

Table 11 Assurance Requirements:EAL2

Assurance Class	Assurance Components
ACM	ACM_CAP.2
ADO	ADO_DEL.1 ADO_IGS.1
ADV	ADV_FSP.1 ADV_HLD.1 ADV_RCR.1
AGD	AGD_ADM.1 AGD_USR.1
ATE	ATE_COV.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_SOF.1 AVA_VLA.1

6. TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 IT Security Functions

This section presents the security functions performed by the TOE and provides a mapping between the identified security functions and the Security Functional Requirements that it must satisfy.

6.1.1 IPSec Implementation

The TOE implements the IETF IPSec protocols (RFCs 2401-2410) to provide confidentiality, authenticity and integrity for packet flows transmitted from and received by the TOE. The TOE IPSec implementation contains a number of functional components that meet the IPSec TSF.

IPSEC.1 - IPSec Internet Key Exchange (IKE)

IKE authenticates IPSec peers (remote TOEs) using pre-shared keys, RSA keys,[1] or digital certificates. It also handles the agreement of secure session keys using the Diffie-Hellman algorithm and negotiates the parameters used during IPSec ESP (IPSEC.2)

IKE maintains a trusted channel, referred to as a Security Association (SA), between IPSec peers that is also used to manage IPSec connections, including:

- The negotiation of mutually acceptable IPSec options between peers,
- The establishment of additional Security Associations to protect packets flows using ESP (as per IPSEC.2), and
- The agreement of secure bulk data encryption (3DES (168-bit) or AES (128, 192, or 256 bit)) keys for use with ESP (IPSEC.2).

IPSEC.2 - IPSec Encapsulating Security Payload (ESP)

The TOE uses ESP to protect packet flows between IPSec peers (instances of the TOE) across intervening untrusted networks in accordance with a TOE security policy (TSP). ESP is a method of encapsulating IP Packets and provides confidentiality using the 3DES and AES ciphers, integrity and authenticity using the MD5 and SHA-1 algorithms, and a mechanism to detect the capture and retransmission of packets (replay attacks).

The parameters used by ESP, including session encryption keys, are negotiated via IPSec security associations (SAs) established via IKE (IPSEC.1) in accordance with the TSP. Note that security associations are unidirectional so that between IPSec peers protecting a packet flow (labelled A and B for example) there are at least two SA's - one from A to B and one from B to A. Each SA, and associated session encryption key, has a lifetime, which upon expiry results in a new SA and session encryption key being established by the SA peers.

The packet flows between two remote IPSec peers that are to be protected by the TOE are defined by way of cryptographic maps (IPSEC.3).

1. Support for RSA public/private key pairs for IKE authentication requires the use of an IPSec hardware acceleration module. Models listed as using "Built In" modules do not support RSA public/private key pairs for IKE authentication.

IPSEC.3 - Cryptographic Maps

Cryptographic Maps are used by the TOE to specify:

a. the packet flow (such as IP packets) that are to be protected by encryption, identified by an access-control list that can include IP protocol, source/destination IP address and source/destination UDP/TCP port number;

b. the IPSec options and parameters to be used when performing encryption;

c. how to identify the peer TOE that will decrypt the packet flow;

d. the interface(s) of the TOE-enabled router that are enabled for IPSec using the parameters specified above.

6.1.2 Packet Filtering

The TOE prevents attempts to establish management control connections to the TOE itself by rejecting packet flows (such as IP packets) that are not consistent with the information flow SFP.

PACKETFILTER.1 - 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.

6.1.3 Configuration and Management

The TOE includes functions that allow the configuration and operation of the security functions of the TOE to be controlled and monitored. The TOE also supports the ability to maintain real time.

CONFIG.1 - System Messages

The TOE generates system diagnostic messages that identify specific TOE operations – errors during IKE negotiation, errors during IPSec processing, whenever a packet matches a filtering rule, and any errors encountered during digital certificate processing. For each event, the TSF shall record the date and time of each event, the type of event, the affected subject identity and the outcome of the event (FAU_AUD.1).

Logged messages for these events can be directed to a combination of an interactive management session, a buffer within the TOE or to an external system outside of the TOE using the SYSLOG protocol. Using the **show logging** command, the authorized user can review the audit messages stored in the buffer on the TOE and act upon them as required. (FAU_SAR.1)

CONFIG.2 - Management Interfaces

The TOE can be configured, managed and operated either via direct local connection to a physical console port, or remotely via an in-band network connection. All management connections must be explicitly enabled to be used, these include:

- Interactive command line interface (CLI) via console or telnet;
- TFTP download of configurations and operating system software;
- Simple Network Management Protocol (SNMP) in read-only mode for monitoring

Interactive CLI connections (console or telnet) require user authentication. The TOE shall be configured to require an access password, which provides unprivileged access and an enable password which provides privileged management access. The unprivileged administrator can only query the TOE configuration. After successful authentication via the CLI interface, an authorized user can upload or download configuration files to/from a TFTP server.

The privileged administrator has control over all TOE functions, attributes, and data, either by executing commands, viewing status and configuration, or editing the TOE configuration settings. The default configuration will be secure so that packet flows will not occur. The privileged administrator has the right to change from the default to allow packet flows.

The TOE will conduct self-tests upon startup to verify that it is operating correctly.

CONFIG.3 - Management of Time

The TOE maintains real time using a reliable software clock that interfaces to an internal hardware clock, or the Network Time Protocol (NTP).

6.1.4 Key Management

To support the authentication of one TOE to another TOE, the TOE supports the use of public key cryptography.

KEYMGT.1 - Key Management

The TOE generates secure RSA public/private keys (512 and 1024 bit key lengths) for use with a Public Key Infrastructure (PKI). The TOE interacts with a certificate authority using the Simple Certificate Enrollment Protocol (SCEP) to download a certificate authority's digital certificate and to request and download a digital certificate for the TOE itself. The TOE can destroy keys it creates by overwriting them.

Table 12 Mapping Summary Specifications to Functional Requirements

TSS Reference	IT Security Function	Function Component	Functional Requirement
IPSEC.1	IPSec Internet Key Exchange (IKE	FCS_CKM.1(2) FTP_ITC.1 FMT_MSA.2	Cryptographic key generation (Diffie Hellman) Inter-TSF trusted channel Secure security attributes
IPSEC.2	IPSec Encapsulating Security Payload (ESP)	FCO_NRO.2 FCS_COP.1 (1) FCS_COP.1 (2) FDP_UCT.1 FDP_UIT.1 FTP_ITC.1	Enforced proof of origin Cryptographic operation (Encryption) Cryptographic operation (Signing) Basic data exchange confidentiality Data exchange integrity Inter-TSF trusted channel

Table 12 Mapping Summary Specifications to Functional Requirements (continued)

TSS Reference	IT Security Function	Function Component	Functional Requirement
IPSEC.3	Cryptographic Maps	FDP_IFC.1 FDP_IFF.1 FTP_ITC.1	Subset information flow control Simple security attributes Inter-TSF trusted channel
PACKETFILTER.1	Packet Filtering	FTA_TSE.1 FDP_IFF.1 FDP_IFC.1	TOE session establishment Simple security attributes Subset information flow control
CONFIG.1	System Messages	FAU_AUD.1[1] FAU_SAR.1 FMT_SMF.1	Audit data generation Audit Review Specification of Management Functions
CONFIG.2	Management Interfaces	FIA_UAU.2 FIA_UAU.5 FIA_UID.2 FMT_SMR.2 FMT_SMR.3 FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FPT_AMT.1 FPT_TST.1 FMT_SMF.1	User authentication before any action Multiple authentication mechanisms User identification before any action Restrictions on security roles Assuming roles Management of security functions behavior Management of security attributes Static attribute initialization Management of TSF data Abstract machine testing TSF testing Specification of Management Functions
CONFIG.3	Management of Time	FPT_STM.1 FMT_SMF.1	Reliable time stamp Specification of Management Functions
KEYMGT.1	Key Management	FCS_CKM.1 (1) FCS_CKM.4 FMT_MSA.2	Cryptographic key generation Cryptographic key destruction Secure security attributes

1. FAU_AUD.1 is a bespoke component based on the [CC] Part 2 component FAU_GEN.1.

6.2 Assurance Measures

The purpose of this section is to show that the identified assurance measures are appropriate to meet the assurance requirements by mapping the identified assurance measures onto the assurance requirements.

The Assurance Measures that demonstrate the correct implementation and use of the Security Functions of the TOE are as follows:

- User Guidance (UG) Documentation
- Functional Specification (FSP) Document
- High Level Design (HLD) Document
- Configuration Management Plan (CMP) Document
- Analysis of Testing (ATE) Document
- Vulnerability Assessment (VA) Document

Table 13 demonstrates that the identified assurance measures completely meet the assurance requirements by showing that all requirements are mapped to an assurance measure.

Table 13 Mapping of Assurance Measures to Assurance Requirements

CC Assurance Component		Assurance Measure
ACM_CAP.2	Configuration Items	Configuration Management Plan
ADO_DEL.1	Delivery Procedures	Configuration Management Plan
ADO_IGS.1	Installation, generation, and start-up procedures	User Guidance
ADV_FSP.1	Information Functional Specification	Functional Specification User Guidance
ADV_HLD.1	Descriptive high-level design	High Level Design
ADV_RCR.1	Informal correspondence demonstration	Functional Specification High Level Design
AGD_AGM.1	Administrator guidance	User Guidance
AGD_USR.1	User guidance	User Guidance
ATE_COV.1	Evidence of coverage	Analysis of Testing
ATE_FUN.1	Functional testing	Analysis of Testing
ATE_IND.2	Independent testing-sample	Analysis of Testing, TOE
AVA_SOF.1	Strength of TOE security function evaluation	Vulnerability Assessment
AVA_VLA.1	Independent vulnerability analysis	Vulnerability Assessment

The assurance measures documents have been specifically written to meet the assurance requirements and are structured as follows:

User Guidance (UG)

- Provides TOE users and administrators with procedural information on installation, configuration and management of the TOE (AGD_USR.1) (AGD_ADM.1)
- Describes procedures for the installation, generation, and start-up of the TOE (ADO_IGS.1)
- Detailed syntax information on the external interfaces used for such interaction with the TOE (ADV_FSP.1)

Functional Specification (FSP)

- Describes the security functionality of the TOE (ADV_FSP.1)
- Defines the external interfaces to the TOE (ADV_FSP.1)
- Demonstrates correspondence with the ST (ADV_RCR.1)

High Level Design (HLD)

- Describes the relationship between TOE sub-systems, their interfaces and the sequence of events in response to stimulus at those interfaces. (ADV_HLD.1)
- Demonstrates correspondence with the FSP (ADV_RCR.1)

Configuration Management Plan (CMP)

- Describes the delivery procedures and how they provide for the detection of modification (ADO_DEL.1)
- Description of TOE generation and acceptance procedures (ACM_CAP.2)

Analysis of Testing (ATE)

- Describes coverage of the testing (ATE_COV.1)
- Describes the testing of security functionality (ATE_FUN.1)
- The TOE will be provided to the evaluators (ATE_IND.2)

Vulnerability Assessment (VA)

- Identifies potential vulnerabilities in the TOE and provides a rationale as to why they are not exploitable in the intended environment for the TOE (AVA_VLA.1).
- Strength of TOE security function evaluation (AVA_SOF.1)

7. PP Claims

This Security Target was not written to conform to any Protection Profile.

8. Rationale

8.1 Security Objectives Rationale

The purpose of the rationale is to demonstrate that the identified security objectives are:

- suitable, they are sufficient to address the security needs;
- necessary, there are no redundant security objectives.

8.1.1 All Assumptions, Policies, and Threats Addressed

Table 14 Cross Reference Objectives to Threats/Assumptions/Policies

Objective / Policy/Threat/Assumption	O.AUTHENTICITY	O.Confidentiality	O.Integrity	O.Key-Confidentiality	O.NoReplay	O.Secure-Operation	OE.Policy	OE.Secure. Management
T.Attack						X		X
T.Untrusted-Path	X	X	X	X	X			
A.PhySec								X
A.NoEvil								X
A.Training								X
A.Trusted-CA								X
A.SecureTimeSource								X
P.Connectivity							X	X

8.1.2 Sufficiency of Security Objectives

Table 15, Table 16, and Table 17 list the sufficiency of the Security Objectives outlined in Table 14.

Table 15 Sufficiency of Security Objectives (1)

Policies	Objectives
P.CONNECTIVITY Rules for Data Flows	The objectives (OE.Policy, OE.Secure-Management) will provide complete coverage as: OE.Policy states that those responsible for the administration of the TOE will be provided with a policy that specifies: **a.** whether the networks which are connected to the TOE are trusted or untrusted, **b.** which packet flows are to be protected by the TOE, and **c.** the peer TOE to be associated with each data flow • OE.Secure-Management states that those responsible for the operation of the TOE will ensure that management and configuration functions of the security functions of the TOE are: **a.** initiated from a management station connected to a trusted network and protected using the security functions of the TOE

Table 16 Sufficiency of Security Objectives (2)

Threat	Objectives
T.ATTACK Unauthorized access	The objectives (O.Secure-Operation, OE.Secure-Management) will provide an effective countermeasure as: • The TOE will be correctly configured in accordance with a security policy which will prevent bypass of the TSF; • The TSP can only be altered by a trusted administrator from a secure management station.
T.UNTRUSTED-PATH Secure transmission of packet flows	The objectives (O.Authenticity, O.Confidentiality, O.Integrity, O.Key-Confidentiality, O.NoReplay) will provide an effective countermeasure as: • O.Authenticity ensures that packet flows are received/transmitted from/to known, authenticated TOEs; • O.Confidentiality ensures that the confidentiality of packet flows is maintained during transmission; • O.Integrity ensures that a packet flow cannot be modified without being detected by the TOE; • O.Key-Confidentiality ensures that cryptographic keys cannot be captured and used to decrypt packet flows; • O.NoReplay ensures that a packet flow transmitted to the TOE has not been copied by an eavesdropper and retransmitted to the TOE.

Table 17 Sufficiency of Security Objectives (3)

Assumption	Objectives
A.PHYSEC TOE will be kept in a physically secure environment.	The objective (OE.Secure-Management) upholds the assumption as: • The TOE will be maintained in a location, which is physically secure.
A.NOEVIL Administrators assumed to be non-hostile and trusted to perform their duties correctly.	The objective (OE.Secure-Management) upholds the assumption as: • Those responsible for the operation of the TOE must ensure that management and configuration of the security functions of the TOE are undertaken by trusted staff trained in the secure operation of the TOE.
A.TRAINING Administrators of the TOE have received training.	The objective (OE.Secure-Management) upholds the assumption as: • Management and configuration of the security functions of the TOE are undertaken by trusted staff trained in the secure operation of the TOE.
A.TRUSTED-CA Digital Certificates are issued from an evaluated/trusted Certificate Authority.	The objective (OE.Secure-Management) upholds the assumption as: • Management and configuration of the security functions of the TOE are implemented in conjunction with an evaluated or trusted Certificate Authority (CA), if digital certificates are used for TOE authentication.
A.SECURETIMESOURCE Sources of time are secure.	The objective (OE.Secure-Management) upholds the assumption as: • Management and configuration of the security functions of the TOE are configured to interface only to trusted clock sources

8.2 Security Requirements Rationale

The purpose of this section is to show that the identified security requirements (See section 5. IT Security Requirements) are suitable to meet the security objectives (See section 4. Security Objectives). The following tables show that each security requirement (and SFRs in particular) is necessary; that is, the tables show that each security objective is addressed by at least one security requirement, and that each security requirement is addressed by at least one security objective.

8.2.1 Functional Security Requirements Rationale

Table 18 Functional Component to Security Objective MappingS

Objective / Requirement	O.AUTHENTICITY	O.Confidentiality	O.Integrity	O.Key-Confidentiality	O.NoReplay	O.Secure-Operation
FAU_AUD.1[1]						X
FAU_SAR.1						X
FCO_NRO.2	X				X	
FCS_CKM.1(1)				X		
FCS_CKM.1(2)				X		
FCS_CKM.4				X		
FCS_COP.1(1)		X				
FCS_COP.1(2)	X		X			
FDP.IFC.1	X	X	X	X		
FDP.IFF.1	X	X	X	X		
FDP_UCT.1		X				
FDP_UIT.1			X			
FIA_UAU.2						X
FIA_UAU.5						X
FIA_UID.2						X
FMT_MOF.1						X
FMT_MSA.1						X
FMT_MSA.2				X		
FMT_MSA.3						X
FMT_MTD.1						X
FMT_SMF.1						X
FMT_SMR.2						X
FMT_SMR.3						X
FPT_AMT.1						X
FPT_STM.1						X
FPT_TST.1						X
FTA_TSE.1						X
FTP_ITC.1	X	X	X	X	X	

1. FAU_AUD.1 is a bespoke component based on the [CC] Part 2 component FAU_GEN.1

Table 19 SFR Sufficiency

Objectives	Requirements
O.AUTHENTICITY Ensure packet flows have been received from a trusted source	The SFRs [FCO_NRO.2, FCS_COP.1(2), FDP_IFC.1, FDP_IFF.1, FTP_ITC.1] are sufficient to satisfy the objective because: • Packet flows received by the TOE must have been digitally signed using the FCO_NRO.2 SFR with key material associated with an identified remote trusted IT product • The FCS_COP.1(2) SFR ensures that the received transmission is digitally signed and therefore its authenticity can be established cryptographically. • The information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1 SFR • The FDP_IFF.1 SFR is used to identify which remote trusted IT product is authenticating which packet flow, and which packet flow is to be authenticated for transmission to a remote trusted IT product • The FTP_ITC.1 SFR establishes a trust relationship with a remote trusted IT product (such as another instance of the TOE).

Table 19 SFR Sufficiency (continued)

Objectives	Requirements
O.CONFIDENTIALITY Protect the confidentiality of packet flows transmitted to/from the TOE over an untrusted network.	The SFRs [FCS_COP.1(1), FDP_UCT.1, FDP_IFC.1, FDP_IFF.1, FTP_ITC.1] are sufficient to satisfy the objective because: • The FCS_COP.1(1) SFR ensures the confidentiality of transmissions through strong encryption. • The FDP_UCT.1 SFR provides confidentiality for packet flows received by, or transmitted from, the TOE using key material associated with an identified remote trusted IT product • The information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1 SFR • The FDP_IFF.1 SFR is used to identify which remote trusted IT product is providing confidentiality for which packet flow, and which packet flow is to be protected when transmitted to a remote trusted IT product • The FTP_ITC.1 SFR establishes a trust relationship with a remote trusted IT product (such as another instance of the TOE)

Table 19 SFR Sufficiency (continued)

Objectives	Requirements
O.INTEGRITY Any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected.	The SFRs [FCS_COP.1(2), FDP_UIT.1, FDP_IFC.1, FDP_IFF.1, FTP_ITC.1] are sufficient to satisfy the objective because: • The FCS_COP.1(2) SFR ensures that the received transmission is digitally signed and therefore its integrity can be established cryptographically. • The FDP_UIT.1 SFR provides integrity for packet flows received by, or transmitted from, the TOE using key material associated with an identified remote trusted IT product • The information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1 SFR • The FDP_IFF.1 SFR is used to identify which remote trusted IT product is providing integrity verification for which packet flow, and which packet flow is to be protected when transmitted to a remote trusted IT product • The FTP_ITC.1 SFR establishes a trust relationship with a remote trusted IT product (such as another instance of the TOE).

Table 19 SFR Sufficiency (continued)

Objectives	Requirements
O.KEY-CONFIDENTIALITY 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 SFRs [FCS_CKM.1 (1), FCS_CKM.1 (2), FCS_CKM.4, FMT_MSA.2, FDP_IFC.1, FDP_IFF.1, FTP_ITC.1] are sufficient to satisfy the objective: • The FCS_CKM.1 SFRs ensures that key generation is robust • FCS_CKM.4 SFR ensures that keys can be safely destroyed • The FCS_CKM.1 (2), SFR ensures that the establishment of the trust relationship and the key agreement operations are cryptographically sound • Cryptographic keys generated are checked to ensure they are secure (FMT_MSA.2) • The information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1 SFR • The FDP_IFF.1 SFR is used to identify which remote trusted IT product is providing integrity verification for which packet flow, and which packet flow is to be protected when transmitted to a remote trusted IT product • The FTP_ITC.1 SFR establishes a trust relationship with a remote trusted IT product (such as another instance of the TOE)

Table 19 SFR Sufficiency (continued)

Objectives	Requirements
O.NOREPLAY Provide a means to detect if an eavesdropper has copied a packet flow and retransmitting it to the TOE.	The SFRs [FCO_NRO.2, FDP_IFC.1, FDP_IFF.1, FTP_ITC.1] are sufficient to satisfy the objective because: • The FTP_ITC.1 SFR establishes a trust relationship with a remote trusted IT product (such as another instance of the TOE) • Packet flows received by the TOE are marked using the FCO_NRO.2 SFR with a sequence number that is uniquely associated with a remote trusted IT product • The information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1 SFR • The FDP_IFF.1 SFR is used to identify which remote trusted IT product is providing integrity verification for which packet flow, and which packet flow is to be protected when transmitted to a remote trusted IT product

Table 19 SFR Sufficiency (continued)

Objectives	Requirements
O.SECURE-OPERATION Prevent unauthorized changes to TOE configuration.	The SFRs [FTA_TSE.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FAU_AUD.1[1], FAU_SAR.1, FMT_MOF.1, FMT_SMF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.2, FMT_SMR.3, FMT_MTD.1, FPT_STM.1, FPT_AMT.1, FPT_TST.1] are sufficient to satisfy the objective because: • The TSF can reject unauthorized session establishments by applying access control lists to deny session establishment, supported by FTA_TSE.1; • The FIA_UAU family supports the requirement for multiple user authentication mechanisms before any actions are carried out on the TSF; • The FIA_UID family supports the requirement to identify the user before any actions are taken on that user's behalf; • The requirements for recording the occurrence of security relevant events that take place under TSF control and the identification of the level of auditing are provided by the FAU_AUD family, and the ability for authorized users to review this audit information is provided by FAU_SAR.1; • The requirement to restrict the ability to determine the behavior of, disable, enable and modify the information flow control SFP is satisfied by FMT_MOF.1; • Authorized users' control over the management of the security attributes is allowed by the FMT_MSA family; • The FMT_SMF.1 requirement specifies the required management functions of the TOE. These management functions includes all user management, packet filtering IPSec and audit configuration. • Control over the assignment of the administrator role to different users is provided by the FMT_SMR family. No user will be able to assume the role of privileged administrator without explicitly requesting and being authenticated as having permission. Users will not be able to assume privileged administrator role unless they have first assumed the administrator role

Table 19 SFR Sufficiency (continued)

Objectives	Requirements
	• The requirement to restrict the ability to query, modify, delete and clear the TSF configuration to privileged administrators is provided by FMT_MTD.1; • The requirement for reliable time-stamps is satisfied by FPT_STM.1; • The requirement for the self-testing of the abstract machine upon which the security functions rely is satisfied by FPT_AMT.1.; • The requirement for self-testing upon startup to verify the proper operation of the TSF code is satisfied by FPT_TST.1

1. FAU_AUD.1 is a bespoke component based on the [CC] Part 2 component FAU_GEN.1.

8.2.2 Suitability of TOE Security Functions to Meet Security Requirements

Table 20 SFR to TSF Cross Reference

TSF / SFR	IPSEC.1	IPSEC.2	IPSEC.3	PACKETFILTER.1	CONFIG.1	CONFIG.2	CONFIG.3	KEYMGT.1
FAU_AUD.1[1]					X			
FAU_SAR.1					X			
FCO_NRO.2		X						
FCS_CKM.1(1)								X
FCS_CKM.1(2)	X							
FCS_CKM.4								X
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						
FDP.IFC.1			X	X				
FDP.IFF.1			X	X				
FDP_UCT.1		X						
FDP_UIT.1		X						
FIA_UAU.2						X		
FIA_UAU.5						X		
FIA_UID.2						X		
FMT_MOF.1						X		
FMT_MSA.1						X		
FMT_MSA.2	X							X
FMT_MSA.3						X		

Table 20 SFR to TSF Cross Reference (continued)

SFR \ TSF	IPSEC.1	IPSEC.2	IPSEC.3	PACKETFILTER.1	CONFIG.1	CONFIG.2	CONFIG.3	KEYMGT.1
FMT_MTD.1						X		
FMT_SMF.1					X	X	X	
FMT_SMR.2						X		
FMT_SMR.3						X		
FPT_AMT.1						X		
FPT_STM.1							X	
FPT_TST.1						X		
FTA_TSE.1				X				
FTP_ITC.1	X	X	X					

1. FAU_AUD.1 is a bespoke component based on the [CC] Part 2 component FAU_GEN.1

FAU_AUD.1

The TSF CONFIG.1 satisfies this requirement by generating audit logs in accordance with the requirement.

FAU_SAR.1

The TSF CONFIG.1 satisfies this requirement by enabling the ability for authorized users to review the audit logs.

FCO_NRO.2

The TSF IPSEC.2 satisfies this requirement by supplying digital signatures on transmitted packets, with which non-repudiation can be established.

FCS_CKM.1 (1)

The TSF KEYMGT.1 satisfies this requirement by providing a mechanism for generating 512 and 1024-bit RSA keys.

FCS_CKM.1 (2)

The TSF IPSEC.1 satisfies this requirement by implementing the Diffie Hellman key agreement algorithm, which allows IPSec peers to agree upon 168-bit 3DES and 128, 192 or 256 bit AES session keys that will be used for bulk encryption.

FCS_CKM.4

The TSF KEYMGT.1 satisfies this requirement by supplying a mechanism for overwriting (destroying) cryptographic keys which the TOE creates.

FCS_COP.1 (1)

The TSF IPSEC.2 satisfies this requirement by providing a mechanism by which data within transmitted packets can be encrypted and decrypted.

FCS_COP.1 (2)

The TSF IPSEC.2 satisfies this requirement by providing a mechanism by which transmitted packets can be digitally signed, and digital signatures can be verified.

FDP_IFC.1

The TSFs IPSEC.3 and PACKETFILTER.1 satisfy this requirement by examining each packet flow and applying the information flow control policy to it.

FDP_IFF.1

The TSFs IPSEC.3 and PACKETFILTER.1 satisfy this requirement by implementing the crypto map function, which permits or deny a packet flow based on its source and destination IP address, and the packetfilter function which is applied to TOE interfaces to implements the information flow control SFP which defines the rules for packet filtering.

FDP_UCT.1

The TSF IPSEC.2 satisfies this requirement by providing encryption of the IP datagram as defined by ESP, thus providing confidentiality.

FDP_UIT.1

The TSF IPSEC.2 satisfies this requirement by providing ESP which signs an IP datagram providing integrity.

FIA_UAU.2

The TSF CONFIG.2 satisfies this requirement by requiring users to undergo authentication before access to its management interfaces is granted.

FIA_UAU.5

The TSF CONFIG.2 satisfies this requirement by requiring a username and password for user authentication, and just an “enable” password for privileged administrator authentication.

FIA_UID.2

The TSF CONFIG.2 satisfies this requirement by requiring users to undergo identification before access to its management interfaces is granted.

FMT_MOF.1

The TSF CONFIG.2 satisfies this requirement by allowing only the privileged administrator the right to manage the functions that implement the information flow control SFP.

FMT_MSA.1

The TSF CONFIG.2 satisfies this requirement by allowing only the privileged administrator the right to manage the configuration that implements the information flow control SFP.

FMT_MSA.2

The TSFs IPSEC.1 and KEYMGT.1 satisfy this requirement in generating only secure cryptographic keys i.e. those that are not weak or semi-weak.

FMT_MSA.3

The TSF CONFIG.2 satisfies this requirement by ensuring that restrictive default values are allocated to security attributes for the Information Flow Control SFP, and allowing the privileged administrator to alter the values from the default.

FMT_MTD.1

The TSF CONFIG.2 satisfies this requirement by only allowing the privileged administrator to alter the TSF configuration

FMT_SMF.1

The TSFs CONFIG.1, CONFIG.2 and CONFIG.3 satisfy this requirement as these TSFs provide all the means with which to interact with the security configuration of the TOE.

FMT_SMR.2

The TSF CONFIG.2 satisfies this requirement by maintaining administrator and privileged administrator roles and ensuring that a user is authenticated as an administrator before allowing them to authenticate as a privileged administrator by using the “enable” password.

FMT_SMR.3

The TSF CONFIG.2 satisfies this requirement by requiring the user to explicitly request using the “enable” command to assume the role of privileged administrator.

FPT_AMT.1

The TSF CONFIG.2 satisfies this requirement by initiating a suite of tests upon startup to ensure proper operation of the underlying abstract machine which underlies the TOE.

FPT_STM.1

The TSF CONFIG.1 satisfies this requirement by monitoring the network time and using the timestamp in audit records.

FPT_TST.1

The TSF CONFIG.2 satisfies this requirement by initiating a suite of tests upon startup to ensure proper operation of the TOE functions.

FTA_TSE.1

The TSF PACKETFILTER.1 satisfies this requirement by examining each packet and discarding those which do not match the access control list it holds.

FTP_ITC.1

The TSFs IPSEC.1, IPSEC.2 and IPSEC.3 satisfy this requirement by authenticating IPSec peers using pre-shared keys, RSA keys or digital certificates and establishing a trusted channel (called Security Associations) for the communication of information with assured identification of end-points; using ESP on IP datagrams to provide confidentiality, authentication, integrity and non-repudiation of sender; and maintaining a cryptographic map which ensures that packet flow source, destination and transmission parameters are controlled

8.2.3 SFR Dependency Rationale

Table 21 shows that the security target has been satisfied SFR’s with dependencies.

Table 21 SFR Dependency Rationale

Requirement	Dependencies
FAU_AUD.1[1]	FPT_STM.1
FAU_SAR.1	FAU_AUD.1
FCO_NRO.2	FIA_UID.2
FCS_CKM.1	FCS_COP.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3
FDP_UCT.1	FTP_ITC.1, FDP_IFC.1
FDP_UIT.1	FDP_IFC.1, FTP_ITC.1
FIA_UAU.2	FIA_UID.2
FIA_UAU.5	N/A
FIA_UID.2	N/A
FMT_MOF.1	FMT_SMF.1, *FMT_SMR.1* (satisfied by FMT_SMR.2)
FMT_MSA.1	FDP_IFC.1, FMT_SMF.1, *FMT_SMR.1* (satisfied by FMT_SMR.2)
FMT_MSA.2	FDP_IFC.1, FMT_MSA.1, *FMT_SMR.1* (satisfied by FMT_SMR.2)
FMT_MSA.3	FMT_MSA.1, *FMT_SMR.1* (satisfied by FMT_SMR.2)
FMT_MTD.1	FMT_SMF.1, *FMT_SMR.1* (satisfied by FMT_SMR.2)
FMT_SMF.1	N/A
FMT_SMR.2	FIA_UID.2
FMT_SMR.3	*FMT_SMR.1* (satisfied by FMT_SMR.2)
FPT_AMT.1	N/A
FPT_STM.1	N/A
FPT_TST.1	FPT_AMT.1
FTA_TSE.1	N/A
FTP_ITC.1	N/A

1. The functional requirement FAU_AUD.1 is based on the [CC] Part 2 functional requirement FAU_GEN.1; thus, it is viewed that FAU_AUD.1 will have a dependency on FPT_STM.1

All functional component dependencies, with the exception of the dependency of FAU_SAR.1 on FAU_GEN.1 are met, as shown in Table 21. The component FAU_SAR.1 is concerned with audit review. The dependency of this component on FAU_GEN.1 relates to the fact that there must be audit events generated in order to review them. As FAU_AUD.1 generates audit events (in much the same way as FAU_GEN.1) it is appropriate to make FAU_SAR.1 dependent upon FAU_AUD.1 rather than FAU_GEN.1.

ADV_SPM.1 is identified as a dependency of FMT_MSA.2, which in turn is identified as a dependency for FCS_CKM.1 (1), FCS_CKM.1 (2), FCS_CKM.4, FCS_COP.1 (1), and FCS_COP.1 (2). The intent of FMT_MSA.2 is that values for security attributes must not violate the TSP. In the context of the FCS family, FMT_MSA.2 requires that the combination of cryptographic security attributes such as key length, key validity period and key use (such as digital signature, key encryption, data encryption) may only be set to values which maintain the 'secure state' of the TOE. By ensuring that the TOE configuration is configured in accordance with the evaluated guidance, the security attributes of the TOE will be set to values which maintain a secure state; therefore, the dependency of FMT_MSA.2 on ADV_SPM.1 is satisfied (as per Section H2, paragraph 1020 of CC v2.3 part 2).

8.2.4 Assurance Security Requirements Rationale

This section shows how the minimum strength of function level for the ST is consistent with the security objectives for the TOE. This ST claims SOF-basic for the strength of function level of the TOE, as

- the TOE is assumed to be physically secure (A.PhySec) and administered by trusted and non-hostile (A.NoEvil) staff with appropriate training (A.Training), and
- the AVA_VLA.2 assurance component, required for EAL2, is considered to be suitable for SOF-basic.

The TOE is intended to be used in environments in which users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. CC Part 3 suggests CC EAL2 as suitable in these circumstances.

8.2.5 Mutually Supportive Security Requirements

The purpose of this rationale is to show that the IT security requirements (and the SFRs in particular) are complete and internally consistent by demonstrating that they are mutually supportive and provide an "integrated and effective whole".

Dependency helps in showing mutual support because if SFR-A is dependent on SFR-B then by definition, SFR-B is supportive of SFR-A. Table 21 shows the dependencies of the Security Functional Requirements.

This ST is targeting a standard EAL 2 assurance package and so the dependency and mutual support of the assurance requirements is self-evident as the EAL is taken from the CC.

Primary and Supporting SFRs

The objectives of the TOE, and the associated SFRs, can be separated into two groups:

1. Those that provide confidentiality, authenticity and integrity for packet flows transmitted and received by the TOE using IPSec (O.Authenticity, O.Confidentiality, O.Integrity, O.Key-Confidentiality, and O.NoReplay). These represent the PRIMARY security enforcing objectives of the TOE, and the associated primary SFRs are listed on the left of Table 22.
2. Those that ensure the TOE can be securely configured, operated and managed (O.Secure-Operation). This is a SUPPORTING objective, and the associated supporting SFRs are listed on the right of Table 22.

The supporting SFRs provide the ability to securely configure, operate and manage the primary SFRs. Therefore, the primary objectives (to protect packet flows) are indirectly provided by the supporting SFRs. Thus, the supporting SFRs provide mutual support for the primary SFRs, as the supporting SFRs help defend the primary SFRs against attacks aimed at defeating the primary SFRs by gaining access to the configuration, operation and management functions of the TOE.

Table 22 Primary and Supporting SFRs

Primary SFRs	Supporting SFRs
FCO_NRO.2, FCS_CKM.1 (1) FCS_CKM.1 (2), FCS_CKM.4, FCS_COP.1 (1), FCS_COP.1 (2), FDP_IFC.1, FDP_IFF.1, FDP_UCT.1, FDP_UIT.1, FTP_ITC.1	FAU_AUD.1[1], FAU_SAR.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, MFT_MTD.1, FMT_SMF.1, FMT_SMR.2, FMT_SMR.3, FPT_AMT.1, FPT_STM.1, FPT_TST.1, FTA_TSE.1

1. FAU_AUD.1 is a bespoke component based on the [CC] Part 2 component FAU_GEN.1.

Help prevent bypassing of other SFRs

FIA_UID.2 and FIA_UAU.2 support other functions that allow the user access to the assets by restricting the actions the user can take before being authorized.

The management function FMT_MSA.1 and FMT_MTD.1 support all other SFRs by restricting the ability to change certain management functions to authorized users, ensuring other users cannot circumvent these SFRs.

FMT_MSA.2 and FMT_MSA.3 limit the acceptable values for secure data, protecting the SFRs dependent on those values from being bypassed.

FPT_AMT.1 and FPT_TST.1 provides for start up and user initiated testing to ensure the security functions are operational, thus preventing their bypass.

FMT_SMF.1 provides for the necessary management functions with which to configure all security functions of the TOE.

Help prevent tampering of other SFRs

The cryptographic functions FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 provide for the secure generation, handling, destruction and operation of keys, and therefore support those SFRs that may rely on the use of those keys.

FDP_UIT.1 supports all other SFRs that deal with data by maintaining data integrity.

FDP_UCT.1 supports all other SFR's that deal with data by maintaining data confidentiality.

FIA_UID.2 and FIA_UAU.2 support other functions that allow the user access to the assets by restricting the actions the user can take before being authorized.

FMT_MSA.1 and FMT_MTD.1 support all other SFRs by restricting the ability to change certain management functions to authorized users, ensuring other users cannot tamper with these SFRs.

FMT_MSA.2 and FMT_MSA.3 limit the acceptable values for secure data, protecting the SFRs dependent on those values from being tampered with.

FPT_AMT.1 and FPT_TST.1 provides for start up and user initiated testing to ensure the security functions are operational, thus checking for tampering.

FMT_SMF.1 provides for the necessary management functions with which to configure all security functions of the TOE.

Help prevent de-activation of other SFRs

The Information Flow Control policy detailed in FDP_IFF.1 along with the primary SFR's identified in table Table 22, provide for rigorous control of allowed data flow, preventing unauthorized deactivation of SFRs.

FMT_MSA.1 and FMT_MTD.1 support all other SFRs by restricting the ability to change certain management functions to authorized users, ensuring other users cannot de-activate these SFRs.

FMT_MSA.2 and FMT_MSA.3 limit the acceptable values for secure data, protecting the SFRs dependent on those values from being de-activated.

FPT_AMT.1 and FPT_TST.1 provides for start up and user initiated testing to ensure the security functions are operational, thus checking for de-activation.

FIA_UID.2 and FIA_UAU.2 support other functions that allow the user access to the assets by restricting the actions the user can take before being authorized.

FTA_TSE.1 supports other functions by allowing the TOE to block the establishment of a user session.

FMT_SMF.1 provides for the necessary management functions with which to configure all security functions of the TOE.

Enable detection of misconfiguration or attack of other SFRs

FAU_AUD.1 and FAU_SAR.1 support other functions by providing logging functions that allow misconfiguration and attacks to be detected.

FPT_AMT.1 supports other functions by providing a reliable timestamp for logging messages.

FMT_SMF.1 provides for the necessary management functions with which to configure all security functions of the TOE

8.2.6 Strength of Function Claims

The National Cryptographic Authority of each CC scheme is the approving authority on strength of cryptographic algorithms. Under these arrangements, the developers can make no claim of strength for cryptographic algorithms. Therefore the explicit strength of function claims for the FCS class of SFR's have been addressed. This also applies to the IT Security Functions IPSEC.1, IPSEC.2, and KEYMGT.1.

For SFR FIA_UAU.5 the strength of function claim is SOF-basic. A Strength of Function claim of SOF-basic is also made for IT Security Function CONFIG.2.

Appendix A—IPSec Operation

IPSec Standards

IPSec combines trusted security technologies into a complete system that provides confidentiality, integrity, and authenticity of IP packets.

These technologies include:

Diffie-Hellman key exchange for deriving key material between SA peers

Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks

Bulk encryption algorithms, such as 3DES or AES, for encrypting the data

Keyed hash algorithms, such as HMAC, combined with traditional hash algorithms such as MD5 or SHA for providing packet authentication

Digital certificates signed by a certificate authority to act as digital ID cards

IPSec itself is broken into two parts:

The IP Security Protocol proper, which defines the information to add to an IP packet to enable confidentiality, integrity, and authenticity controls as well as defining how to encrypt the packet data. The TOE uses the IPSec Encapsulating Security Payload (ESP) in IPSec Tunnel mode.

Internet Key Exchange (IKE), which negotiates the security association between two entities and exchanges key material. It is not necessary to use IKE, but manually configuring security associations is a difficult and manually intensive process. IKE should be used in most real-world applications to enable large-scale secure communications.

Figure 8 IPSec Tunnel Mode

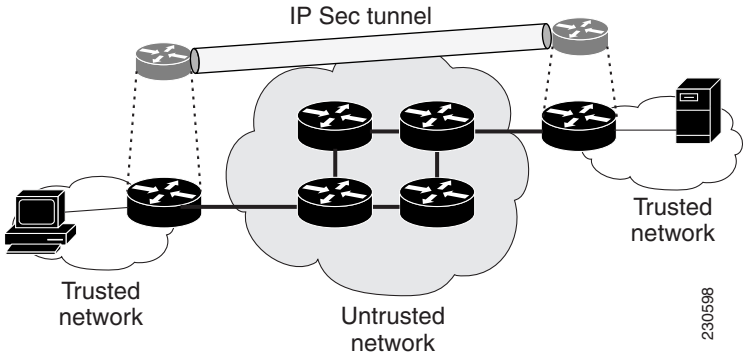
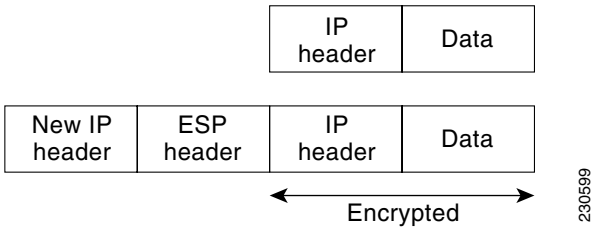


Figure 9 IPSec Encapsulating Security Payload



IPSec Security Associations

IPSec provides many options for performing network encryption and authentication. The TOE requires encryption, integrity and authentication. When the security service is determined, the two communicating nodes must determine exactly which algorithms to use (the TOE uses 3DES or AES for encryption; and SHA-1 for integrity). After deciding on the algorithms, the two devices must share session keys. The security association is the method that IPSec uses to track all the particulars concerning a given IPSec communication session. A Security Association (SA) is a relationship between two or more IPSec devices that describes how the entities will use security services to communicate securely.

An IPSec security association is unidirectional, meaning that for each pair of communicating IPSec devices there are at least two security connections - one from A to B and one from B to A. The security association is uniquely identified by a randomly chosen unique number called the security parameter index (SPI) and the destination IP address of the destination. When a system sends a packet that requires IPSec protection, it looks up the security association in its database, applies the specified processing, and then inserts the SPI from the security association into the IPSec header. When the IPSec peer receives the packet, it looks up the security association in its database by destination address and SPI and then processes the packet as required.

A special bi-directional SA, known as the IKE SA is used to establish and manage all IPSec SA's.

IPSec Operation

Authentication

IKE creates an authenticated, secure tunnel between two IPSec entities (such as the TOE) called the IKE SA, which is then used to negotiate the security associations for IPSec used to protect the packet flow. This process requires that the two entities authenticate themselves to each other and establish shared keys. IKE supports multiple authentication methods. The two entities must agree on a common authentication protocol through a negotiation process. The following mechanisms are supported in the TOE:

Pre-shared key

The same key is pre-installed on each device. IKE peers authenticate each other by computing and sending a keyed hash of data that includes the preshared key. If the receiving peer is able to independently create the same hash using its preshared key, it knows that both parties must share the same secret, thus authenticating the other party

Public key cryptography

Each party generates a pseudo-random number (a nonce) and encrypts it in the other party's public key. The ability for each party to compute a keyed hash containing the other peer's nonce, decrypted with the local private key as well as other publicly and privately available information, authenticates the parties to each other. This system provides for deniable transactions. That is, either side of the exchange can plausibly deny that it took part in the exchange. Currently only the RSA public key algorithm is supported.

Digital signature

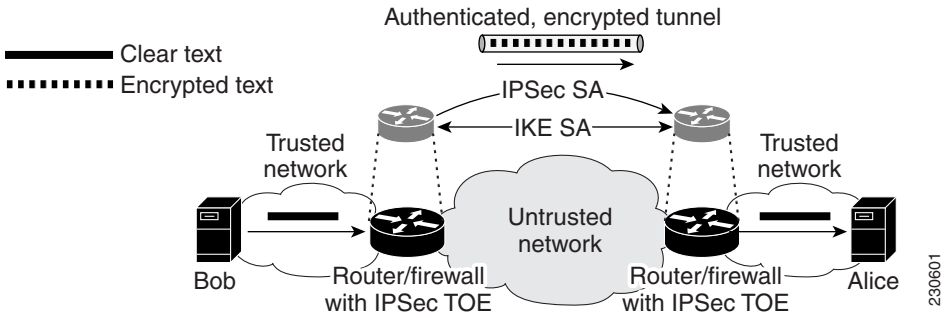
Each device digitally signs a set of data and sends it to the other party. This method is similar to the previous one, except that it provides nonrepudiation. Currently both the RSA public key algorithm and the digital signature standard (DSS) are supported.

Key Exchange

Both parties must have a shared session key in order to encrypt the IKE tunnel. The Diffie-Hellman protocol is used to agree on a common session key. The exchange is authenticated as described above to guard against “man-in-the-middle” attacks.

These two steps, authentication and key exchange, create the IKE SA, a secure tunnel between the two devices. One side of the tunnel offers a set of algorithms, and the other side must then accept one of the offers or reject the entire connection. When the two sides have agreed on which algorithms to use, they must derive key material to use for IPSec with Authentication Headers (AH), ESP (Encapsulating Security Payload), or both together (the TOE uses ESP only). IPSec uses a different shared key than IKE. The IPSec shared key can be derived by using Diffie-Hellman again to ensure perfect forward secrecy, or by refreshing the shared secret derived from the original Diffie-Hellman exchange that generated the IKE SA by hashing it with pseudo-random numbers (nonces). The first method provides greater security but is slower. After this is complete, the IPSec SA is established and the packet flow is passed over the IPSec SA.

Figure 10 IPSec and IKE Operation



For example, in Figure 10, Bob is trying to securely communicate with Alice. Bob sends his data (IP packets) toward Alice. When Bob’s internetworking device sees the packet, it checks its security policy and realizes that the packet should be encrypted. The preconfigured security policy also says that Alice's internetworking device will be the other endpoint of the IPSec tunnel. Bob’s internetworking device looks to see if it has an existing IPSec SA with Alice’s internetworking device. If not, then it negotiates one using IKE. If the two internetworking devices already share an IKE SA, the IPSec SA can be quickly and immediately generated. If they do not share an IKE SA, one must first be created before negotiation of the IPSec SAs. As part of this process, the two internetworking devices exchange authentication credentials, such as digital certificates. A certificate authority that both Bob and Alice’s internetworking devices trust must sign the certificates beforehand. When the IKE session becomes active, the two internetworking devices can negotiate the IPSec SA. When the IPSec SA is set up, both internetworking

devices will have agreed on an encryption algorithm (for example, 3DES) and an authentication algorithm (for example, SHA), and have a shared session key. Now, Bob's internetworking device can encrypt Bob's IP packet, place it into a new IPSec packet and send it to Alice's internetworking device. When Alice's internetworking device receives the IPSec packet, it looks up the IPSec SA, properly processes and unpacks the original datagram, and forwards it over to Alice. Note that this process is transparent to both Alice and Bob.