

**Security Target
for
Cisco Remote Access VPN**

Reference: ST
16 May 2007
Version 1.17

CISCO Systems Inc.
170 West Tasman Drive
San Jose
CA 95124-1706
USA

Copyright: ©2007 Cisco Systems, Inc.

Table of Contents

Conventions	6
Terminology	6
Document Organisation	7
1 INTRODUCTION	8
1.1 Identification	8
1.2 Security Target Overview	8
1.3 CC Conformance Claims	9
2 TOE DESCRIPTION	10
2.1 Product Type	10
2.1.1 VPN Clients.....	10
2.1.1.1 Software VPN Client.....	10
2.1.1.2 Hardware VPN Client	11
2.1.2 VPN Concentrators	12
2.1.3 Authentication Server	14
2.2 General TOE Functionality	14
2.2.1 IPSec	15
2.2.2 Access Controls	17
2.2.3 Configuration and Management	18
2.3 Scope and Boundaries	18
2.3.1 Logical	18
2.3.2 Physical	20
2.4 Application Notes	20
2.4.1 Remote Access VPN.....	20
2.4.2 Secure Intranet VPN	21
3 ENVIRONMENT	23
3.1 Assumptions	23
3.2 Threats	24

4	OBJECTIVES	25
4.1	TOE Security Objectives.....	25
4.2	Environmental Security Objectives	25
5	REQUIREMENTS	27
5.1	TOE Security Functional Requirements	27
5.1.1	Audit Review (FAU_SAR.1).....	27
5.1.2	Cryptographic key generation (FCS_CKM.1/RSA).....	27
5.1.3	Cryptographic key generation (FCS_CKM.1/DES).....	27
5.1.4	Cryptographic key generation (FCS_CKM.1/AES).....	27
5.1.5	Cryptographic key generation (FCS_CKM.1/HMAC).....	27
5.1.6	Cryptographic key destruction (FCS_CKM.4).....	27
5.1.7	Cryptographic operation (FCS_COP.1/Encryption).....	28
5.1.8	Cryptographic operation (FCS_COP.1/Signing).....	28
5.1.9	Cryptographic operation (FCS_COP.1/Auth).....	28
5.1.10	Complete access control (FDP_ACC.2)	28
5.1.11	Security Attribute Based Access Control (FDP_ACF.1).....	28
5.1.12	Complete information flow control (FDP_IFC.2).....	29
5.1.13	Simple security attributes (FDP_IFF.1).....	29
5.1.14	Basic data exchange confidentiality (FDP_UCT.1)	30
5.1.15	Data exchange integrity (FDP_UIT.1).....	30
5.1.16	User Attribute Definition (FIA_ATD.1/Users)	30
5.1.17	User Attribute Definition (FIA_ATD.1/Admin)	30
5.1.18	User authentication before any action (FIA_UAU.2).....	30
5.1.19	Multiple authentication mechanisms (FIA_UAU.5)	30
5.1.20	User identification before any action (FIA_UID.2).....	30
5.1.21	Management of security functions behaviour (FMT_MOF.1).....	30
5.1.22	Management of security attributes (FMT_MSA.1/Conf)	31
5.1.23	Management of security attributes (FMT_MSA.1/Keys)	31
5.1.24	Secure security attributes (FMT_MSA.2).....	31
5.1.25	Static attribute initialisation (FMT_MSA.3).....	31
5.1.26	Security roles (FMT_SMR.1).....	31
5.1.27	Assuming roles (FMT_SMR.3).....	31
5.1.28	Reliable time stamps (FPT_STM.1)	31
5.1.29	TOE session establishment (FTA_TSE.1)	31
5.1.30	Inter-TSF trusted channel (FTP_ITC.1/Client)	32
5.1.31	Inter-TSF trusted channel (FTP_ITC.1/AuthSvr).....	32
5.2	Explicitly Stated TOE Security Functional Requirements	32
5.2.1	Audit data generation (FAU_AUD.1).....	32
5.3	Security Requirements on the Environment	33
5.3.1	Cryptographic key generation (FCS_CKM.1/TOK_RSA)	33
5.3.2	Cryptographic key destruction (FCS_CKM.4/TOK).....	33
5.3.3	Cryptographic operation (FCS_COP.1/TOK_Auth)	33
5.3.4	User authentication before any action (FIA_UAU.2/TOK).....	33

5.3.5	User identification before any action (FIA_UID.2/TOK)	33
5.3.6	Management of security attributes (FMT_MSA.1/TOK_Keys)	33
5.3.7	Secure security attributes (FMT_MSA.2/TOK)	34
5.4	TOE Security Assurance Requirements	34
6	SECURITY FUNCTIONS	35
6.1	TOE Security Functions	35
6.1.1	IPSec Implementation	35
6.1.1.1	IPSec.Auth (IPSec Authentication – IKE)	35
6.1.1.2	IPSec.Encrypt (IPSec Encryption – ESP)	36
6.1.2	Filtering Controls	36
6.1.2.1	Filtering.Interface (VPN Concentrator Interface Access Control)	36
6.1.2.2	Filtering.Client (VPN Client Access Control)	36
6.1.2.3	Filtering.SplitControl (VPN Client Split Tunnelling)	36
6.1.3	Management	37
6.1.3.1	Mgt.Conc (VPN Concentrator Configuration and Operation)	37
6.1.3.2	Mgt.Client (VPN Client Configuration and Operation)	37
6.1.3.3	Mgt.AuthServ (Authentication Server Configuration and Operation)	38
6.1.3.4	Mgt.User (Management of Groups and Users)	38
6.1.3.5	Mgt.CertMgt (Digital Certificate Management)	38
6.1.3.6	Mgt.EventLog (Logging of Events)	39
6.1.3.7	Mgt.Clock (Maintenance of Time)	39
7	RATIONALES	40
7.1	Security Objectives Rationale	40
7.2	Requirements Rationales	45
7.3	TOE Summary Specification Rationales	50
7.4	Assurance Measures	58
7.4.1	User Guidance (UG)	58
7.4.2	Design Specification (DS) Documents	58
7.4.3	Configuration Management Procedures (CMP)	58
7.4.4	Analysis of Testing (ATE)	58
7.4.5	Vulnerability Assessment (VA)	59
7.5	Security Assurance Requirements Rationale	59
7.6	Functional Dependencies	59
7.7	Mutual Support	60
7.7.1	Mutual Support of SFRs	60
7.7.1.1	Help prevent bypassing of other SFRs	60
7.7.1.2	Help prevent tampering of other SFRs	60
7.7.1.3	Help prevent de-activation of other SFRs	61

7.7.1.4	Enable detection of misconfiguration or attack of other SFRs.....	61
7.7.2	Mutual Support of TSFs.....	61
7.8	Strength of Function Rationale.....	62

Conventions

The notation, formatting and conventions used in this Security Target are consistent with those used in Version 2.1 of the Common Criteria (CC). 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 Section 2.1.4 of Part 2 of the CC. Refinements are indicated by **bold text** for inserted words and ~~strike through~~ for removed words.

Terminology

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

CC	Common Criteria
EAL	Evaluation Assurance Level
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
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 following terminology specific to the TOE and its environment is also provided to aid the user of the Security Target.

ESP	Encapsulating Security Payload
HMAC	Hashed Message Authentication Code
IETF	Internet Engineering Task Force

IKE	Internet Key Exchange
MD5	Message Digest 5
MODECONF	Mode Configuration
NTP	Network Time Protocol
PKI	Public Key Infrastructure
RFC	Request For Comment; a standards document of the IETF
SCEP	Simple Certificate Enrolment Protocol
SHA	Secure Hash Algorithm
VPN	Virtual Private Network
XAUTH	Extended Authentication
The Administrator	The administrator is an account with full privileges to manage the TOE.
Privileged Administrator	An administrative account with privileges to perform TOE administrative functions, which have been allowed by the administrator.
Administrators	Refers to the use of both the administrator and privileged administrator.

Document Organisation

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 3, respectively that must be satisfied by the TOE.

Section 6 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 7 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements

1 Introduction

1.1 Identification

Title: Security Target for Cisco Remote Access VPN, Version 1.17

Author: Cisco Systems Inc.

Last Updated: 16 May 2007

CC Version: 2.1 Final

Keywords: VPN, IPsec, VPN3000

1.2 Security Target Overview

The TOE is an integrated solution of hardware and software components that allow trusted IT systems to securely communicate with a trusted network over an untrusted network. Virtual Private Network (VPN) VPN Client software installed on the trusted IT systems is used to authenticate and encrypt data exchanged with the trusted network via a VPN Concentrator. The VPN Concentrator validates connections using authentication credentials stored internally, or externally on an Authentication Server. The TOE also includes hardware VPN Clients.

The TOE is called the Cisco Remote Access VPN. The components of the TOE are:

Component	Description	Version	Supported Operating Systems
Software VPN Clients	Cisco VPN Client for Windows	4.8.00.0440	Windows XP Professional v2002 with SP2
	Cisco VPN Client for Linux	4.8.00(0490)	Redhat Linux 3.2.2-5 Kernel version 2.4.20-8
	Cisco VPN Client for Solaris	4.6.02(0030)	Solaris 10 for SPARC (Sun 5.10)
	Movian VPN Client for Pocket PC (developed by Certicom Corporation)	4.00 Build 113.12c	Pocket PC 2002 v3.0.11171
	Movian VPN Client for Palm OS (developed by Certicom Corporation)	4.00 Build 112.15P	Garret v.5.4.9 PalmOS
	AnthaVPN Client for Windows CE .NET (developed by Certicom Corporation)	5.6.2	Windows CE .NET 4.20
Hardware VPN Clients	Cisco VPN 3002 and 3002-8E Hardware VPN Clients	4.7.2.D	N/A (Integrated)
	Cisco PIX 501	6.3(5)	N/A (Integrated)
	Cisco 831 and 837 routers	12.4(5a) (fc3)	N/A (Integrated)

Component	Description	Version	Supported Operating Systems
VPN Concentrator	Cisco VPN 3005 and 3015 Concentrators	4.1.7.N	N/A (Integrated)
VPN Concentrator with Scalable Encryption Processor(s) (SEPs)	Cisco VPN 3020, 3030, 3060 and 3080 Concentrators	4.1.7.N	N/A (Integrated)
Authentication Server	CiscoSecure ACS	4.0(1) Build 27	Windows Server 2003 standard ed
SEPs	Scaleable Encryption Processor	SEP-E	4.0

Table 1-1 Evaluated Versions of the TOE Components

1.3 CC Conformance Claims

The TOE is CC (Version 2.1) Part 2 extended, and will conform to EAL2 measures in Part 3 of the CC (Version 2.1).

2 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 contains three components:

1. VPN Clients (software, and hardware appliances)
2. VPN concentrators (hardware appliance)
3. Authentication server (software)

These are shown in Figure 2-1.

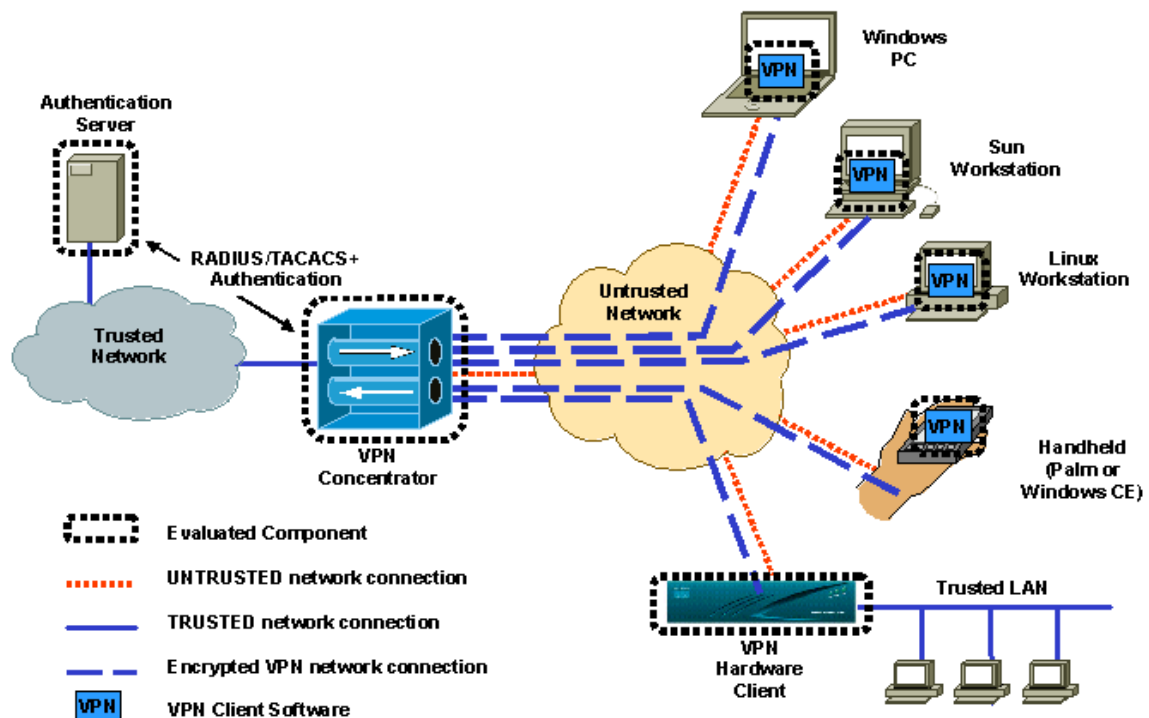


Figure 2-1 TOE Components

2.1.1 □ VPN Clients

The TOE includes a range of VPN Clients both software and hardware.

2.1.1.1 Software VPN Client

The software VPN Clients are used when a single trusted IT system requires a secure connection to a trusted network over an untrusted network, and the trusted IT system

uses one of the operating systems supported by the software VPN Clients (see Table 1-1). Examples of trusted IT systems include:

- PCs or Notebooks running the Windows XP Professional operating system,
- PCs running the Redhat Linux operating system,
- Sun workstations running the Solaris operating system,
- Symbol VRC8900 Series Vehicle Mount Devices running the Windows CE .NET operating system, and
- Handheld computers running the Pocket PC or PalmOS operating systems.

The VPN Client software is installed on an existing trusted IT system and implements the authentication and encryption functions required by the TOE.

2.1.1.2 Hardware VPN Client

The hardware VPN Client is used to:

- a) Securely connect a single trusted IT system that does not use one of the operating systems supported by the software VPN Clients to a trusted network over an untrusted network, or
- b) Securely connect a single trusted LAN of trusted IT systems to a trusted network over an untrusted network.

The hardware VPN Client is a fixed configuration network appliance with an imbedded proprietary operating system. There are three hardware VPN Clients; the Cisco VPN 3002 (which has two different physical models), the Cisco 830 series router (which has two different physical models, the 831 and 837) and the Cisco PIX 501 as shown in Figure 2-2.

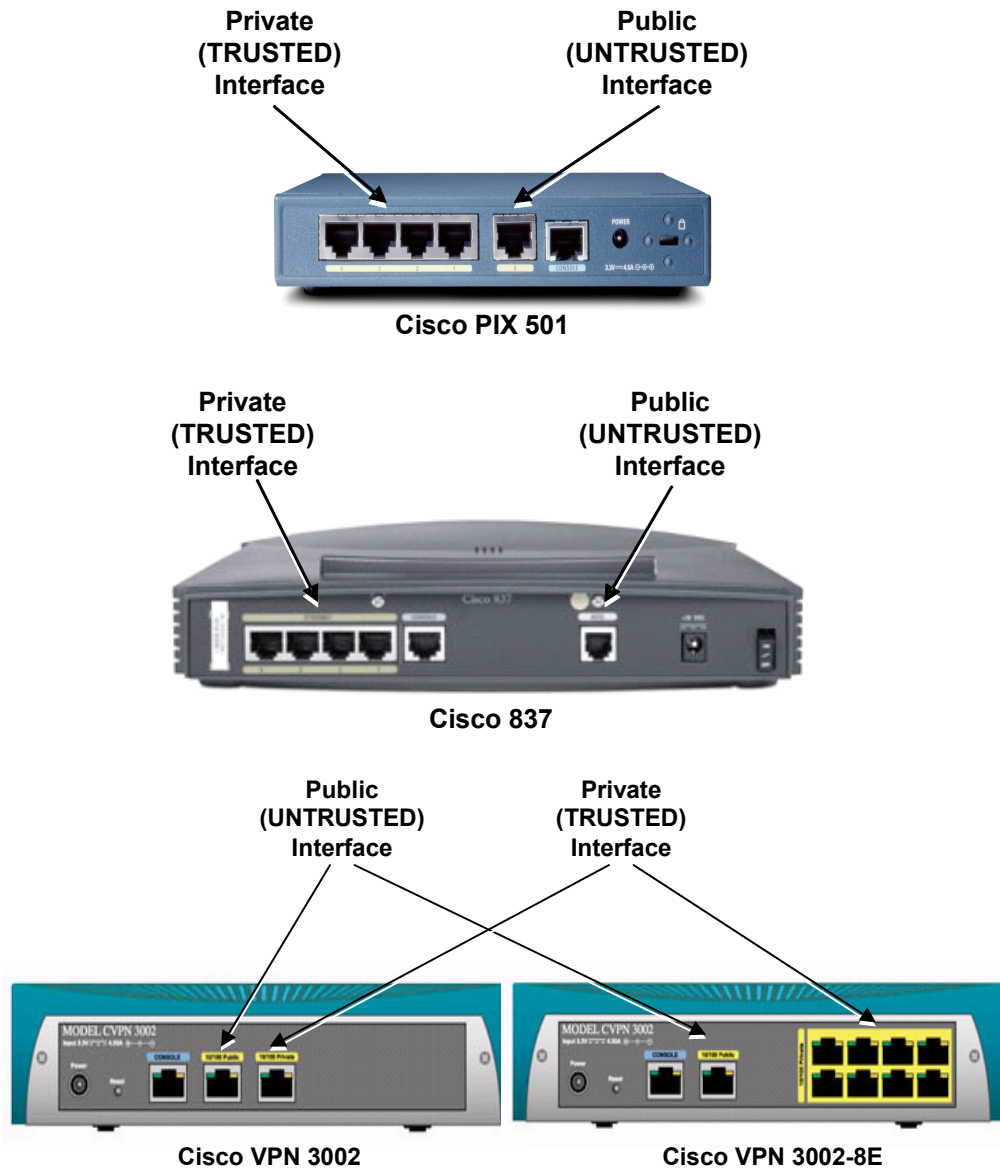


Figure 2-2 Hardware VPN Clients Types and Models (rear)

All hardware VPN Clients have a Public interface that is connected to the untrusted network, and a Private interface that is connected to the trusted LAN or IT system. Note that the VPN3002-8E model has an integrated 8 port LAN switch, and the Cisco 830 series and the PIX 501 have an integrated 4 port LAN switch in place of the private interface, to allow the direct connection of up to 8 and 4 trusted IT systems respectively.

2.1.2 □ VPN Concentrators

The VPN concentrator is a network appliance with an imbedded proprietary operating system.

The VPN Concentrator terminates secure connections established across an untrusted network from trusted IT systems equipped with the VPN Client (described in section

2.1.1) to provide access to a trusted network. The VPN concentrator has two physical interfaces; one connected to an untrusted network and the other connected to a trusted network (see Figure 2-3).

There are six models of the VPN concentrator included within the TOE as detailed in Table 2-1.

	VPN3005	VPN3015	VPN3020	VPN3030	VPN3060	VPN3080
Number of VPN Clients	100	100	750	1,500	5,000	10,000
Encryption	Software	Software	Hardware	Hardware	Hardware	Hardware
Installed SEPs	None	0	1	1	2	4
Spare SEP Slots	None	4	None	3	2	0

Table 2-1 VPN Concentrator Models

The VPN3005 is a fixed configuration model with no expansion slots and performs all cryptographic operations in software (Figure 2-3).

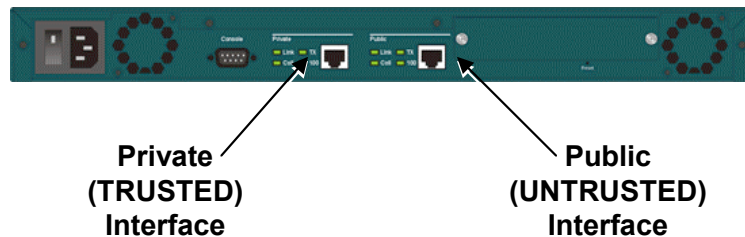


Figure 2-3 Cisco VPN 3005 Chassis (rear)

The VPN3015, VPN3020, VPN3030, VPN3060 and VPN3080 models share a common modular chassis with four slots for Scalable Encryption Processors (SEPs) to accelerate cryptographic processing using dedicated hardware. A maximum of two SEPs are in use at any time – additional SEPs provide redundancy.

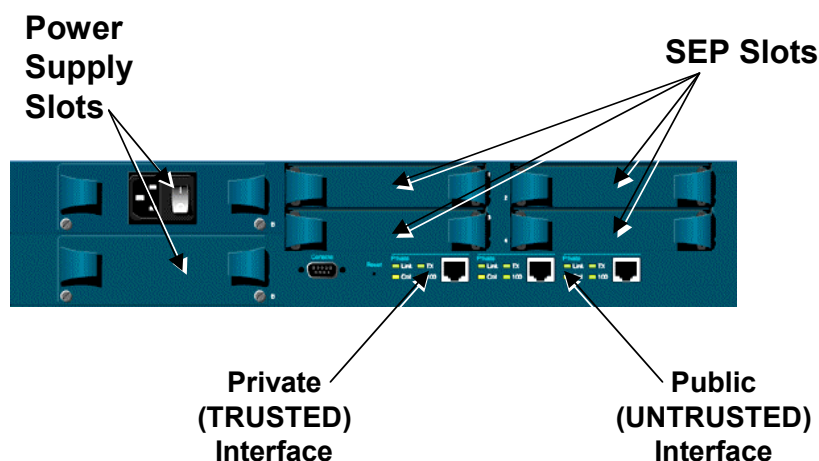


Figure 2-4 Cisco VPN 3015, 3020, 3030, 3060, 3080 Chassis (rear)

2.1.3 □ Authentication Server

The TOE includes an Authentication Server that can be used to store authentication credentials to validate connections from VPN Clients to the VPN Concentrator.

The Authentication Server is the CiscoSecure ACS (Access Control Server) application installed on a Windows 2003 Server system. The Authentication Server is connected to the trusted network side of the VPN Concentrator and accepts and responds to requests to validate group names/passwords and usernames/passwords from the VPN Concentrator using the RADIUS authentication protocol. The Authentication Server also accepts and responds to requests to validate administrator usernames/passwords from the VPN Concentrator using the TACACS+ authentication protocols.

2.2 General TOE Functionality

The primary security function of the TOE is the implementation of IPSec to provide confidentiality, authenticity and integrity services for connections across an untrusted network from trusted VPN Clients to a trusted network via a VPN Concentrator. Other components and functions of the TOE support this primary function.

The VPN concentrator authenticates connections from VPN Clients using group names/passwords or digital certificates, and/or username/passwords (including One Time Passwords). Group names/passwords and username/passwords can be maintained on the VPN concentrator, or on an Authentication Server (section 2.1.3) with which the VPN concentrator communicates using the RADIUS authentication protocol. Detailed configuration options relating to the operation of the VPN Client are configured on the VPN concentrator and downloaded to the VPN Client once the VPN Client has been authenticated and a secure connection established.

The software VPN Client software intercepts all TCP/IP data between the trusted IT systems TCP/IP stack and network interfaces to determine whether the data must be encrypted/decrypted (see Figure 2-5). The VPN Client also performs authentication using a group name/password or a digital certificate, and/or a username/password (including One Time Passwords). The VPN Client for Windows operating systems supports the use of a SmartCard or token to store these authentication credentials.

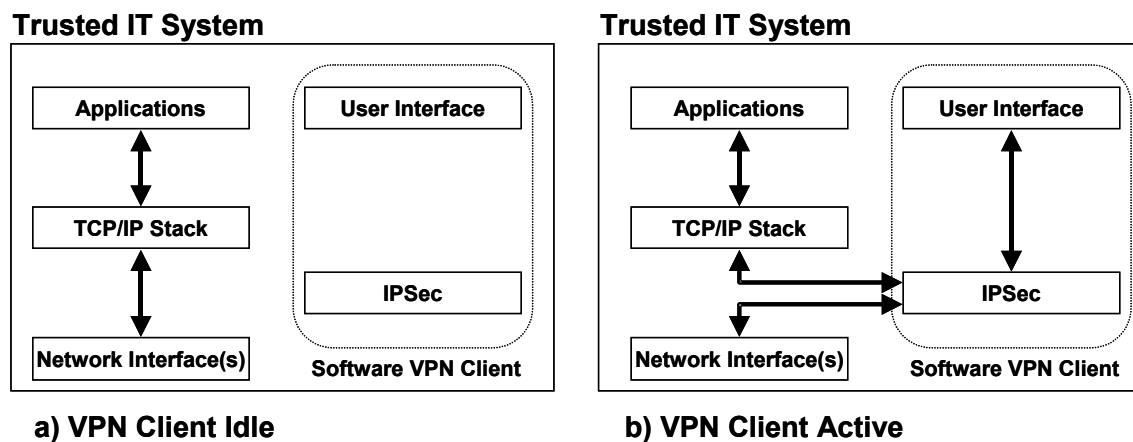


Figure 2-5 Software VPN Client Overview

The hardware VPN Client performs encryption/decryption on behalf of one of more trusted IT systems connected to its private (trusted) interface. The VPN Client is configured with the necessary credentials (group name/password, username/password and/or digital certificate) to authenticate itself to the VPN Concentrator.

The remainder of this section describes the IPSec functionality that is supported by the TOE, and the specific TOE functions that support IPSec

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.

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 therefore 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.

Within the TOE, IPSec is implemented in both the VPN Concentrator and the VPN Clients (see section 2.1). IPSec connections are initiated by the VPN Clients to the VPN concentrator to enable the VPN Client system to securely participate in a trusted network across an untrusted network.

The TOE supports the IPSec options detailed in Table 2-2.

Function	IPSec Options
Authentication between VPN Clients and VPN Concentrator	IPSec Internet Key Exchange (IKE) using: <ul style="list-style-type: none"> • Pre-shared keys (group names/passwords) with XAUTH¹ (usernames/passwords), • Digital Certificates with XAUTH (usernames/passwords), or • Digital Certificates stored on SmartCards/Tokens Group names/passwords and Usernames/passwords can be stored on the VPN Concentrator or on the TOE Authentication Server
Confidentiality of Data between VPN Client and VPN Concentrator	IPSec Encapsulating Security Payload (ESP) Tunnel Mode using: <ul style="list-style-type: none"> • 168 bit 3DES (Triple DES), or • 128, 192, or 256 bit AES
Integrity and Authenticity of Data between VPN Client and VPN Concentrator	IPSec Encapsulating Security Payload (ESP) with Hashed Message Authentication Code (HMAC) in Tunnel Mode using: <ul style="list-style-type: none"> • SHA-1, or • MD-5

Table 2-2 IPSec Options Supported by TOE

Not all authentication mechanisms are supported by all VPN Clients. The authentication mechanisms supported by each of the TOE VPN Clients is shown in Table 2-3.

¹ XAUTH – Extended Authentication. An IETF draft that specifies username/password authentication as an extension to IKE

VPN Client	Operating System	Group name/password with Username/password	Digital Certificate	
			with Username/Password	stored on SmartCard/Token
Cisco VPN Software Clients	Windows	✓	✓	✓
	Linux	✓	✓	
	Solaris	✓	✓	
Movian VPN Software Clients	Pocket PC	✓		
	Palm OS	✓		
Anthavpn Software Client	Windows CE .NET	✓		
Cisco Hardware VPN Clients	VPN 3002	✓	✓	
	VPN 3002-8E	✓	✓	
	PIX 501	✓	✓	
	Cisco 830	✓	✓	

Table 2-3 TOE VPN Client Authentication Options

2.2.2 □ Access Controls

The VPN Concentrator supports the ability to filter inbound packets on both the private and public interfaces based on source/destination IP address, IP protocol, and TCP/UDP source/destination port number (ie. application). This allows the VPN Concentrator to only accept packets that are VPN Client authentication requests, IPSec encrypted or to/from a trusted source (eg. Authentication Server). This is particularly important for the public interface as it is generally connected to an untrusted network and allows the VPN Concentrator to be “self defending” and reject unauthorised connection attempts.

All VPN Clients are connected to the untrusted network to gain connectivity to the VPN Concentrator. When a secure tunnel from the VPN Client is established to the VPN Concentrator, the VPN Client is also connected to the trusted network. To prevent the VPN Client being used as a conduit for attackers on the untrusted network attempting to access to the trusted network when the secure tunnel is in place, the VPN Client can disable the trusted IT system’s access to the untrusted network when the secure tunnel is established. This is often called disabling split tunnelling. The VPN Concentrator controls this function during the establishment of the secure tunnel to the VPN Client.

The VPN Concentrator can enforce further access controls on connections from VPN Clients by applying a filter based on source/destination IP address, IP protocol, and TCP/UDP source/destination port number (ie. application) to data received over secure tunnels from VPN Clients. Filters can be configured per user or per group. This allows VPN Clients to be permitted or denied access to specific networks, hosts or services within the trusted network.

2.2.3 □ Configuration and Management

The software VPN Client must be installed on a trusted IT system and configured with the authentication credentials and connection details necessary to authenticate the VPN Client to the appropriate VPN Concentrator. Specific IPSec parameters and other configurations options for the software VPN Client are downloaded from the VPN concentrator after successful authentication.

Initial bootstrap configuration of the VPN Concentrator must be performed using the VPN Concentrator's console port and hence requires direct physical access. Further configuration, operation and management are carried out via an in-band Web-based interface. To ensure that only authorised administrators can gain secure access to this interface, the TOE specifies that an administrator must first authenticate by entering an administrator username/password.

Initial bootstrap configuration of the hardware VPN Client is carried out over a console port and hence also requires direct physical access. This initial set-up process includes the configuration of authentication credentials and connection details necessary to authenticate the VPN Client to the appropriate VPN Concentrator. Specific IPSec parameters and other configurations options for the hardware VPN Client are downloaded from the VPN concentrator after successful authentication.

The VPN Concentrator manages users of the TOE in terms of users and groups. All users must be members of a group, and all groups are members of a base group. IPSec parameters and other configuration options can be inherited by a group from the base-group and by users from a group, or configured specifically for a user or group. The group and user database can be maintained on the VPN Concentrator or on an Authentication Server. The VPN Concentrator communicates with the Authentication Server using the RADIUS protocol.

The Authentication Server is configured and managed via a web-based GUI that is username and password protected.

2.3 Scope and Boundaries

2.3.1 □ Logical

The TOE is an interoperable collection of functions implemented in several hardware and software components. The TOE only addresses:

- The IPSec function, which provides confidentiality, authenticity, and integrity for connections across an untrusted network from the VPN Client to the VPN Concentrator, and

- Functions that support the secure configuration and operation of the IPSec function, including access controls, configuration and management.

This is illustrated in Figure 2-6 TOE Logical Boundaries with Hardware VPN Client (TOE elements shaded)

and Figure 2-7 TOE Logical Boundaries with Software VPN Client (TOE elements shaded)

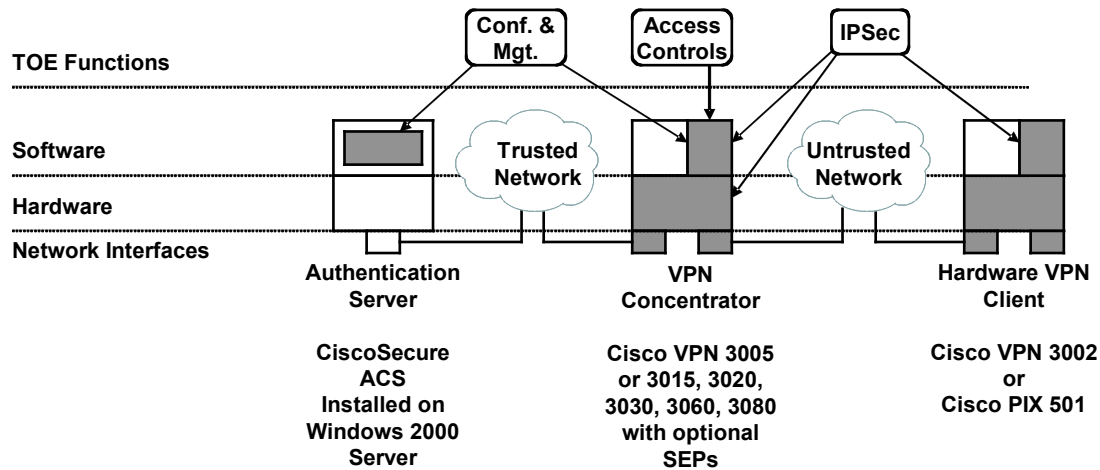


Figure 2-6 TOE Logical Boundaries with Hardware VPN Client (TOE elements shaded)

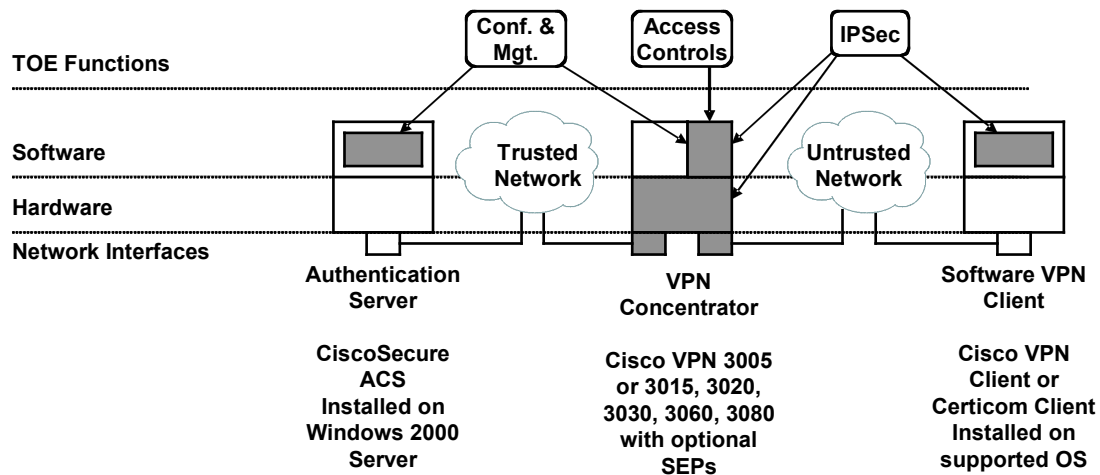




Figure 2-7 TOE Logical Boundaries with Software VPN Client (TOE elements shaded)

The software VPN Client and Authentication Server components of the TOE are applications that are resident on a trusted IT system within an associated host operating system (as indicated by ).

The hardware VPN Client and VPN Concentrator are dedicated devices with purpose written software whose primary function is the implementation of the IPSec function. They also support many other functions, some of which are included within the scope of the TOE (such as access controls, configuration and management), and others that are outside the scope of the TOE (such as VPN Client addressing) (as indicated by .

2.3.2 □ Physical

The following physical boundaries are defined within the TOE:

- A software VPN Client is contained on a trusted IT system and connected to the untrusted network via some form of network interface, under the control of the host operating system, eg. LAN, dialup, or wireless. When active, the software VPN Client provides confidentiality, authenticity, and integrity for traffic transmitted over the untrusted network to a VPN Concentrator.
- A hardware VPN Client is connected to both the untrusted network via its public interface, and a local trusted LAN network via its private interface. The hardware VPN Client provides confidentiality, authenticity, and integrity for traffic transmitted by any systems connected to the local trusted LAN over the untrusted network to a VPN Concentrator.
- The VPN Concentrator is connected to both the untrusted network via its public interface, and a central trusted network via its private interface. The VPN Concentrator authenticates secure connections from VPN Clients across the untrusted network.
- The Authentication Server is connected to the central trusted network via some form of network interface, under the control of the host Windows Server 2003 operating system, usually a LAN interface. The Authentication Server receives authentication requests and responds to them over the central trusted network.

2.4 Application Notes

The TOE defined by the ST is used to provide secure access to a trusted network over an untrusted network. The most common application of this capability is to provide a Remote Access Virtual Private Network (VPN), typically over the Internet. Another common application is to provide internal (Intranet) connections over an untrusted physical medium such as a wireless network, creating a secure Intranet VPN.

2.4.1 □ Remote Access VPN

The TOE enables travelling, remote and telecommuting employees to access a corporate Intranet over the Internet or other untrusted IP network. An example showing the TOE deployed within an Internet access firewall is shown in Figure 2-8. Two options are shown for integrating the VPN Concentrator with a firewall. Option A shows the VPN Concentrator public (untrusted network) interface connected to the Internet access router, using the TOE access control functions to limit connections to the VPN Concentrator to secure connections from VPN Clients.

Option B shows the VPN Concentrator public (untrusted network) interface connected to a firewall interface. This allows the firewall to enforce limited access controls on behalf of the VPN Concentrator, in addition to the TOE access control functions. Note however that traffic to the public interface will be encrypted and hence the firewall can not inspect protocol or application data from the VPN Client. With both options, the VPN Concentrator private (trusted network) interface is connected to a dedicated interface in the firewall, allowing firewall policy to be configured for connections from VPN Clients on one interface and for general Internet access on the other.

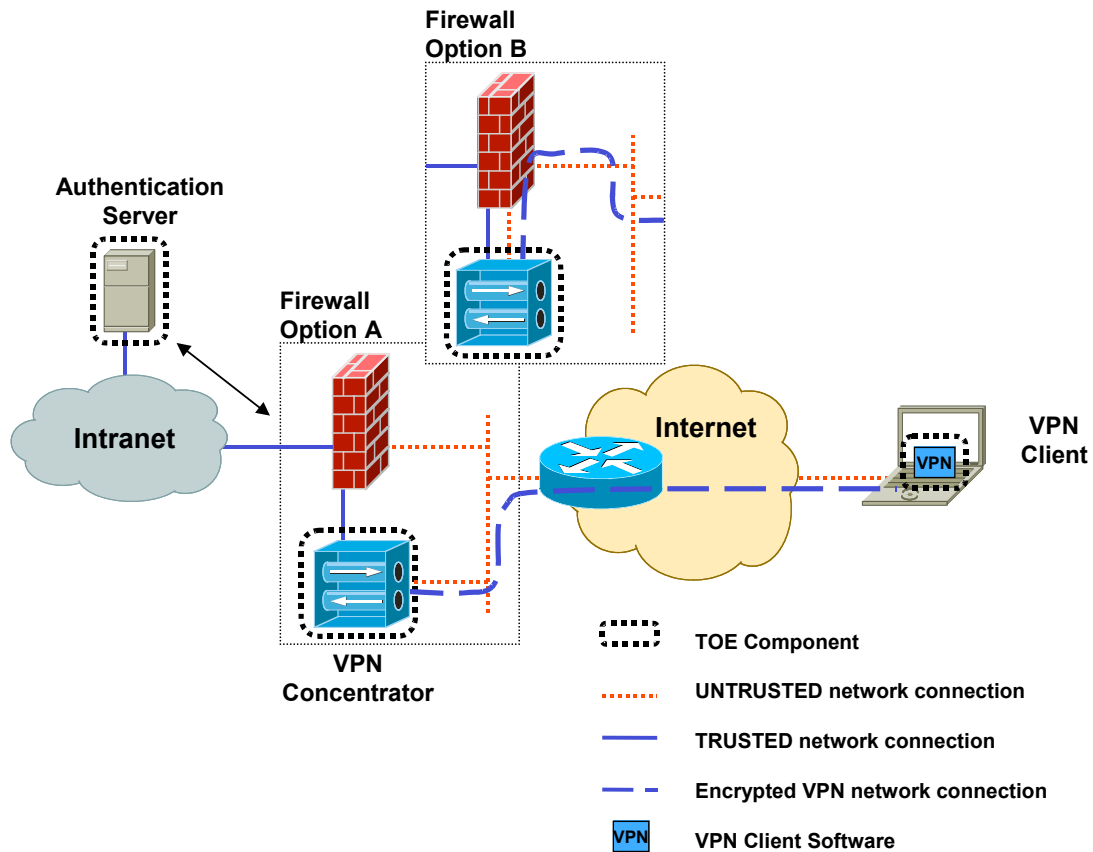


Figure 2-8 Remote Access VPN

2.4.2 □ Secure Intranet VPN

The TOE enables systems that are connected to untrusted or unapproved physical infrastructure to access a corporate Intranet. An example based on a wireless LAN is shown in Figure 2-9. In this scenario the VPN Concentrator's public (untrusted network) interface is connected to a wireless LAN base station supporting wireless connections to VPN Clients. Using the functions of the TOE, the VPN Clients are able to establish secure connections over the wireless LAN to the Intranet connected to the VPN Concentrator's private (trusted network) interface.

Note that some wireless LAN standards include mechanisms to secure connections between wireless VPN Clients and the base station. For example, within the 802.11b standard the Wired Equivalent Privacy (WEP) mechanism uses the RC4 encryption algorithm to secure VPN Client-base station communication. The TOE overlays this capability to provide an evaluated solution based on the 3DES/AES algorithms (which is a requirement in some deployments).

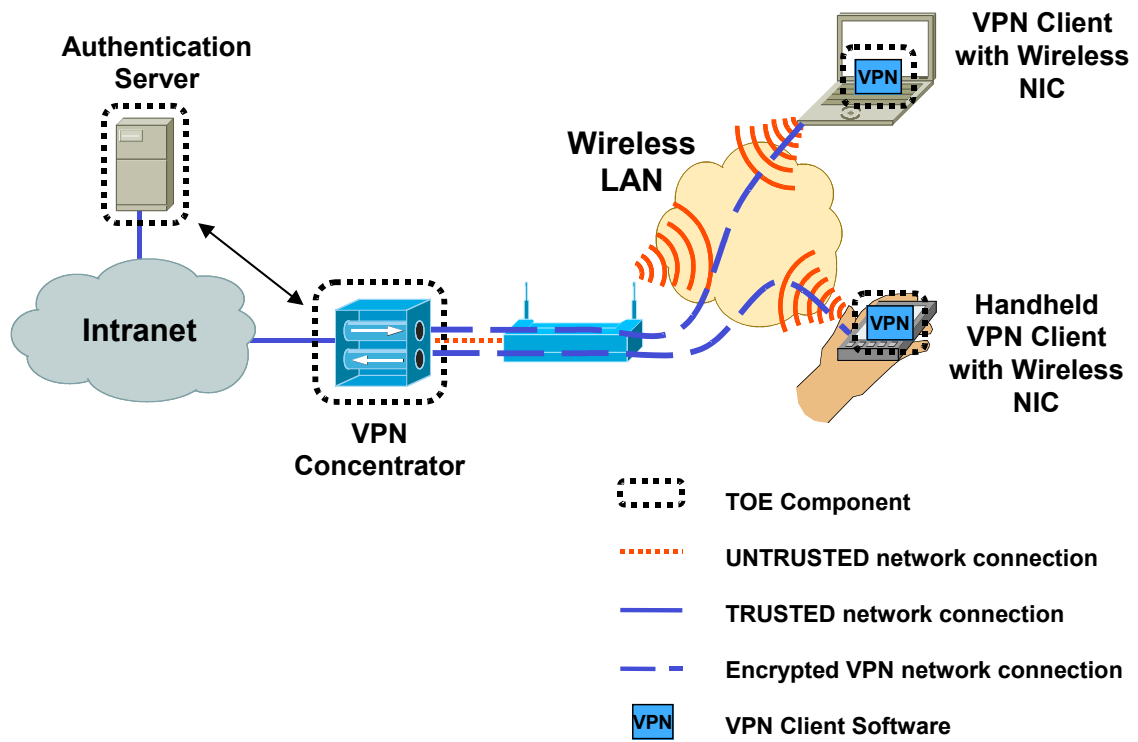


Figure 2-9 Secure Wireless Intranet VPN

3 Environment

In order 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/or 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 organisational security policy statements or rules with which the TOE must comply.

3.1 Assumptions.

Following are assumptions that are required for the TOE to remain secure and carry out the TSFs.

A.Network	The trusted network is appropriately protected against unauthorised access and usage.
A.Admin	Administrators will configure the TOE as defined in the Installation and Configuration Guidance.
A.Users	Users are trusted to follow the security Practises and Policies that apply on the trusted network.
A.Passwords	Administrators will configure the TOE with passwords that are at least eight characters long, and of appropriate complexity. NOTE: This version of VPN 3000 software only supports passwords constructed from letters A – Z; a – z; and numerals 0 – 9.
A.OS	The operating systems that support the Software VPN Clients operate as specified.
A.Con-Physical	The VPN Concentrator and trusted network are physically secure.
A.LAN-Physical	The Hardware VPN Client and trusted LAN are physically secure.
A.Soft-Secure	The Software VPN Client will be installed on a trusted IT system and operated in a physically secure manner.
A.Token	Smart Cards or USB tokens and their readers and drivers behave as specified, can be trusted to protect the certificates and private keys that they hold and do not provide any services to the TOE without the user first being authenticated by the token.
A.Certificates	If certificates are being used by the TOE, the certificate authority and processes associated with the issuance and revocation of certificates are trusted.
A.Remote	The TOE will be configured to require remote management sessions over the untrusted network to be encrypted.

3.2 Threats.

The Threat agents against the TOE are attackers with a low attack potential, i.e. Attackers with high resources, high skill and low motivation.

- | | |
|-----------------|--|
| T.Snoop | An attacker may attempt to obtain data being transmitted between the VPN Client and trusted network by viewing traffic. |
| T.Configuration | An attacker (whether an insider or outsider) may gain access to the TOE and compromise its security functions by altering its configuration. |
| T.Authenticate | An attacker may attempt to gain authentication credentials of a VPN Client to allow access to the protected network. |
| T.Insert | An attacker may attempt to place data on the internal network by inserting it into a valid packet flow. |
| T.Modify | An attacker may attempt to place data on the internal network by modifying a valid packet flow. |
| T.SplitTunnel | An attacker located on an untrusted network may gain access to the internal network via the VPN Client when a valid, open connection exists between the VPN Client and VPN Concentrator. |
| T.UserAccess | An authenticated VPN Client may gain access to internal network resources that they are not authorised to access. |

4 Objectives

These objectives define the TOE and what it will achieve.

4.1 TOE Security Objectives.

O.UserAuth	All users and administrators of the TOE must be authenticated.
O.Secure	All traffic between the TOE VPN concentrator and the TOE VPN Clients must be securely encrypted and signed.
O.EAL	The TOE must be tested and shown to be resistant to obvious vulnerabilities.
O.ConfigAccess	The TOE will allow access to the configuration of the TOE VPN concentrator to the administrator roles only.
O.Roles	The TOE shall maintain roles for Privileged Administrator, Administrators and Users.
O.PacketFilter	The TOE will filter inbound traffic to ensure that only user traffic is accepted by the VPN concentrator.
O.SplitControl	The TOE will restrict connections to/from the VPN Client from/to an untrusted network when an encrypted connection is established.
O.Audit	The TOE will generate audit records for events related to the functionality of the TOE and provide means to review the generated records.
O.ClientControls	The TOE will filter connections established by VPN Clients to limit access to internal network resources.

4.2 Environmental Security Objectives

OE.UserAuth	The smart card Token supporting the TOE will ensure users are authenticated prior to performing any actions on behalf of the TOE.
OE.Users	The users of the TOE are trained in and understand the Security Policies for their trusted network/s.
OE.Administrators	The administrators of the TOE will be trained in the operation of the TOE and understand and comply with the Security Policies of the trusted network/s.
OE.ClientOS	The operating systems that support the VPN Client software are securely configured and maintained.
OE.Certificates	The Certificate processes implemented to support the TOE will be trusted.

OE.Token

The smart card Token employed to support the TOE will be trusted to protect user credentials.

5 Requirements

5.1 TOE Security Functional Requirements

The TOE functional security requirements contained within Section 5.1 are drawn from [CC] Part 2.

5.1.1 Audit Review (FAU_SAR.1)

The TSF shall provide [administrator or authorised privileged administrators] with the capability to read [all audit information] from the audit records.^{FAU_SAR.1.1}

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

Application Note: Privileged Administrators have the ability to perform administrative functions as defined by the administrator.

5.1.2 Cryptographic key generation (FCS_CKM.1/RSA)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [512, 768, 1024, 2048 bits] that meet the following: [RFC 2409].^{FCS_CKM.1.1}

5.1.3 Cryptographic key generation (FCS_CKM.1/DES)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Diffie-Hellman] and specified cryptographic key sizes [168 bits] that meet the following: [RFC 2405].^{FCS_CKM.1.1}

5.1.4 Cryptographic key generation (FCS_CKM.1/AES)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Diffie-Hellman] and specified cryptographic key sizes [128, 192, 256 bits] that meet the following: [RFC 3394].^{FCS_CKM.1.1}

5.1.5 Cryptographic key generation (FCS_CKM.1/HMAC)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [HMAC] and specified cryptographic key sizes [128, 160 bits] that meet the following: [RFC 2409].^{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 specified standard].^{FCS_CKM.4.1}

5.1.7 □ Cryptographic operation (FCS_COP.1/Encryption)

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

5.1.8 □ Cryptographic operation (FCS_COP.1/Signing)

The TSF shall perform [digital signing] in accordance with a specified cryptographic algorithm [HMAC in conjunction with MD5 and SHA-1] and cryptographic key sizes [128, 160 bits respectively] that meet the following: [RFC2049, MD5 and SHA-1].^{FCS_COP.1.1}

5.1.9 □ Cryptographic operation (FCS_COP.1/Auth)

The TSF shall perform [certificate verification] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [512, 768, 1024, 2048 bits] that meet the following: [RFC 2409].^{FCS_COP.1.1}

5.1.10 Complete access control (FDP_ACC.2)

The TSF shall enforce the [access control policy] on [

Subjects: All users

Objects: VPN Concentrator configuration data]

and all operations among subjects and objects covered by the SFP.^{FDP_ACC.2.1}

The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.^{FDP_ACC.2.2}

5.1.11 Security Attribute Based Access Control (FDP_ACF.1)

The TSF shall enforce the [access control policy] to objects based on [administrator authentication credentials and administrator permissions.]^{FDP_ACF.1.1}

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [an administrator is authenticated and the operation is allowed by administrator permissions.]^{FDP_ACF.1.2}

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [Access to the administrative functions is always allowed to the administrator when identified and authenticated].^{FDP_ACF.1.3}

The TSF shall explicitly deny access of subjects to objects based on the [following rules:

- Access to privileged administrator permission configuration is denied to all users except the administrator; and

- Access to the AES and HMAC keys, and RSA private keys is denied for all users of the VPN Concentrator. The VPN Concentrator may only read the keys when it is performing cryptographic functions.].^{FDP_ACF.1.4}

5.1.12 Complete information flow control (FDP_IFC.2)

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

subjects: VPN Clients on the untrusted network; and

a trusted network,

information: Data from the trusted network to a VPN Client on the untrusted network]

and all operations that cause that information to flow to and from subjects covered by the SFP^{FDP_IFC.2.1}

The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.^{FDP_IFC.2.2}

5.1.13 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: [

- Source/destination IP address;
- Source/destination port number; and
- Authentication credentials as specified in FIA_UAU.5.]^{FDP_IFF.1.1}

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [rules configured by an administrator based on security attributes.]^{FDP_IFF.1.2}

The TSF shall enforce the [none.]^{FDP_IFF.1.3}

The TSF shall provide the following [none.]^{FDP_IFF.1.4}

The TSF shall explicitly authorise an information flow based on the following rules: [the authentication credentials provided by the VPN Client can be successfully validated; and

Received packet flows identified by source/destination IP address and source/destination port number are permitted (accepted) by the configured filtering and split tunnelling rules.]^{FDP_IFF.1.5}

The TSF shall explicitly deny an information flow based on the following rules: [the authentication credentials provided by the VPN Client cannot be successfully validated; or

Received packet flows identified by source/destination IP address and source/destination port number are denied (dropped) by the configured filtering and split tunnelling rules.]^{FDP_IFF.1.6}

5.1.14 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 unauthorised disclosure.^{FDP_UCT.1.1}

5.1.15 Data exchange integrity (FDP_UIT.1)

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

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

5.1.16 User Attribute Definition (FIA_ATD.1/Users)

The TSF shall maintain the following list of security attributes belonging to individual users: [Authentication Credentials, Filters]^{FIA_ATD.1.1}

5.1.17 User Attribute Definition (FIA_ATD.1/Admin)

The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ **administrators**: [Authentication Credentials and Privileges]^{FIA_ATD.1.1}

5.1.18 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}

5.1.19 Multiple authentication mechanisms (FIA_UAU.5)

The TSF shall provide [

- Group names and group passwords (shared keys) or
- Digital Certificates, and optionally,
- Username names and user passwords]

to support user authentication.^{FIA_UAU.5.1}

The TSF shall authenticate any user's claimed identity according to the [rules specified by administrators].^{FIA_UAU.5.2}

5.1.20 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}

5.1.21 Management of security functions behaviour (FMT_MOF.1)

The TSF shall restrict the ability to [disable, enable, and modify the behaviour of] the functions [that implement the access control SFP] to [privileged administrators].^{FMT_MOF.1.1}

5.1.22 Management of security attributes (FMT_MSA.1/Conf)

The TSF shall enforce the [access control SFP] to restrict the ability to [query, modify and delete] the security attributes [configuration data] to [privileged administrator.]^{FMT_MSA.1.1}

5.1.23 Management of security attributes (FMT_MSA.1/Keys)

The TSF shall enforce the [access control SFP] to restrict the ability to [generate or install] the security attributes [VPN concentrator encryption keys] to [the TOE] and [VPN concentrator authentication keys] to [the TOE or privileged administrator.]^{FMT_MSA.1.1}

5.1.24 Secure security attributes (FMT_MSA.2)

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

Application Note: This SFR relates to the acceptance of cryptographic keys for use within the TOE. The TOE will generate secure keys as defined in RFCs 2405 (3DES), 3394 (AES) and 3447 (RSA).

5.1.25 Static attribute initialisation (FMT_MSA.3)

The TSF shall enforce the [access 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}

5.1.26 Security roles (FMT_SMR.1)

The TSF shall maintain the roles: [administrator, privileged administrator, and user].^{FMT_SMR.1.1}

The TSF shall be able to associate users with roles.^{FMT_SMR.1.2}

5.1.27 Assuming roles (FMT_SMR.3)

The TSF shall require an explicit request to assume the following roles: [any role].^{FMT_SMR.3.1}

5.1.28 Reliable time stamps (FPT_STM.1)

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

5.1.29 TOE session establishment (FTA_TSE.1)

The TSF shall be able to deny session establishment based on [IP protocol, Source and/or destination IP addresses, and/or TCP/UDP Port].^{FTA_TSE.1.1}

5.1.30 Inter-TSF trusted channel (FTP_ITC.1/Client)

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 [~~selection: the TSF, the remote trusted IT Product~~] VPN **Clients** 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 VPN Clients and trusted networks].^{FTP_ITC.1.3}

5.1.31 Inter-TSF trusted channel (FTP_ITC.1/AuthSvr)

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 [~~selection: the TSF, the remote trusted IT Product~~] VPN **Concentrator** to initiate communication via the trusted channel.^{FTP_ITC.1.2}

The TSF shall initiate communication via the trusted channel for [the authentication of users, when the VPN Concentrator is configured to use the Authentication Server].^{FTP_ITC.1.3}

5.2 Explicitly Stated TOE Security Functional Requirements

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 start-up 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 start-up and shutdown redundant.

This function has a dependency on FPT_STM.1 to provide time stamping of audit records. This dependency is satisfied by the TOE.

5.2.1 Audit data generation (FAU_AUD.1)

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

- Attempted User Authentication;
- Attempted VPN Client Authentication (IKE);
- IPSEC status (enabled/disabled);
- IPSEC ESP Tunnel established (Failure only);
- VPN Concentrator Reboot;
- Manual Time Change (Success only);
- Daylight Saving Time Change (Success only);
- NTP Time Change Attempt;

- Telnet connection established;
- SNMP session established; and
- HTTP connection attempted.

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

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

5.3 Security Requirements on the Environment

The TOE Microsoft Windows client can operate with certificates stored on evaluated (Smart Card or USB) tokens. This section is provided to describe the SFRs being met by the environment in this instance.

If the TOE is configured to use certificates on a token, the token is required to implement the following requirements from CC part 2.

5.3.1 Cryptographic key generation (FCS_CKM.1/TOK_RSA)

The ~~TSF~~ **Token** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [512, 768, 1024 or 2048 bits] that meet the following: [PKCS #1].^{FCS_CKM.1.1}

5.3.2 Cryptographic key destruction (FCS_CKM.4/TOK)

The ~~TSF~~ **Token** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [no specific standard].^{FCS_CKM.4.1}

5.3.3 Cryptographic operation (FCS_COP.1/TOK_Auth)

The ~~TSF~~ **Token** shall perform [certificate verification] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [512, 768, 1024, or 2048 bits] that meet the following: [PKCS #1].^{FCS_COP.1.1}

5.3.4 User authentication before any action (FIA_UAU.2/TOK)

The ~~TSF~~ **Token** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.^{FIA_UAU.2.1}

5.3.5 User identification before any action (FIA_UID.2/TOK)

The ~~TSF~~ **Token** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.^{FIA_UID.2.1}

5.3.6 Management of security attributes (FMT_MSA.1/TOK_Keys)

The Token shall enforce the [access control SFP] to restrict the ability to [generate or install] the security attributes [VPN Client authentication keys] to [the Token's authenticated user].^{FMT_MSA.1.1}

5.3.7 Secure security attributes (FMT_MSA.2/TOK)

The ~~TSE~~ **Token** shall ensure that only secure values are accepted for security attributes.^{FMT_MSA.2.1}

Application Note: This SFR relates to the acceptance of cryptographic keys for use within the TOE. The Token will generate secure keys as defined in 3447 (RSA).

5.4 TOE Security Assurance Requirements

The TOE meets all the Assurance Requirements prescribed by EAL2 in Part 3 of the CC.

6 Security Functions

This section presents the Security Functions implemented by the TOE.

6.1 TOE Security Functions

6.1.1 IPsec Implementation

The VPN concentrator and VPN Client elements of the TOE implement the IPsec protocol to provide confidentiality, authenticity and integrity for packet flows passing between the VPN concentrator and the VPN Client over an untrusted network. The implementation of IPsec by these elements of the TOE contains the following functional components.

6.1.1.1 IPsec.Auth (IPsec Authentication – IKE)

The Internet Key Exchange protocol (IKE) is used to authenticate TOE VPN Clients to the TOE VPN concentrator. IKE is also used to establish and maintain the connections between the VPN Client and VPN concentrator that perform encryption of user data (see IPsec.Encrypt, 6.1.1.2). The generation of DES, AES and HMAC keys for use in IPsec.Encrypt is implemented using a Diffie-Hellman exchange and the HMAC key generation standard as part of IKE. The primitives used to generate the keys are overwritten with a sequence of bits when the ESP tunnel is terminated.

Authentication is minimally based on either pre-shared keys (configured as a group name and group password) or digital certificates as per [IKE]. Authentication can be further refined by requiring that a username and user password be supplied as defined in [XAUTH].

The combination of group name/password or digital certificate, and optional username/password are either statically configured into the VPN Client or requested by the VPN Client using an interactive prompt at connection time, then securely transmitted from the VPN Client to the VPN concentrator for verification.

The VPN concentrator validates connections from the VPN Client using a combination of

- A digital certificates installed on the VPN concentrator (see 6.1.3.5, Mgt.CertMgt)
- group names/passwords configured on the VPN concentrator or the Authentication Server (see 6.1.3.4, Mgt.User)
- usernames/passwords configured on the VPN concentrator or the Authentication Server (see 6.1.3.4, Mgt.User)

as required.

For this evaluation, the required combination of authentication credentials is one of the following:

- Group name/password AND Username/password;
- Certificate stored on VPN Client AND Username/password; OR

- Certificate stored on a trusted token or VPN Hardware Client.

6.1.1.2 IPsec.Encrypt (IPsec Encryption – ESP)

The Encapsulation Security Payload (ESP) provides confidentiality, integrity, and authenticity for packet flows when added to an IP datagram. Confidentiality is implemented using the 3DES and AES ciphers. Integrity and authenticity are implemented using HMAC digital signature standard to sign MD5 or SHA-1 message digests.

The TOE VPN Client and VPN concentrator use ESP to encrypt packet flows over the untrusted network between them. The DES, AES and HMAC keys are overwritten with a sequence of bits when the ESP tunnel is terminated.

ESP uses sequence numbers within a maintained sliding window to detect the insertion of unauthorised packets into an authorised packet flow or the unauthorised replaying of packets from an authorised packet flow.

6.1.2 □ Filtering Controls

The TOE VPN concentrator prevents attempts to connect to the VPN Concentrator itself, the VPN Client or other IT resources that are not consistent with the flow control SFP.

6.1.2.1 Filtering.Interface (VPN Concentrator Interface Access Control)

The TOE VPN Concentrator performs input packet filtering by applying filters to its private (trusted) and public (untrusted) interfaces. The filter can include IP protocol, source/destination IP address and source/destination UDP/TCP port number. Packets received on an interface that do not matching the filter are counted, optionally logged and discarded by the VPN Concentrator. Access to the configuration for this function is controlled by the Mgt.Conc function.

6.1.2.2 Filtering.Client (VPN Client Access Control)

A filter can be enabled at the VPN concentrator that performs input packet filtering on user data arriving via the secure connection (or tunnel) from the VPN Client. The filter can include IP protocol, source/destination IP address and source/destination UDP/TCP port number. Packets received on an interface that do not match the filter are logged and discarded by the VPN Concentrator. This allows connections from the VPN Client to the trusted network to be constrained to specific sub networks, hosts, and/or services within the trusted network. This control mechanism can be configured on a per group basis, and if username/password authentication is enabled, on a per username basis (see Section 6.1.3.4, Mgt.User).

6.1.2.3 Filtering.SplitControl (VPN Client Split Tunnelling)

The TOE VPN Concentrator restricts which networks the VPN Client can access when a secure connection has been established (also called split tunnelling) by

applying a filter to the VPN Client Interface. The filter restricts access to remote networks based on the destination IP prefix.

6.1.3 □ 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 applies authentication and access controls consistent with the access control SFP by maintaining a repository containing authentication credentials and configuration attributes.

To support the authentication of VPN Clients by the VPN concentrator, the TOE supports the use of public key cryptography using digital certificates.

6.1.3.1 Mgt.Conc (VPN Concentrator Configuration and Operation)

The TOE VPN Concentrator requires that administrators identify and authenticate themselves prior to allowing access to configuration attributes that control the operation of the TOE VPN Concentrator. Administrator accounts require a user name and password combination that matches a combination stored on the VPN Concentrator or the TOE Authentication Server. The TOE must be configured to use one of these two authentication stores to authenticate administrative users. If the Authentication Server is used, the VPN Concentrator will request authorisation of an administrative user by forwarding the supplied logon credentials to the Authentication Server using the TACACS+ authentication protocol. The remote server will respond with an access authorised or access denied. A specific remote server will be configured to Authenticate users and authentication will fail if it is not available.

The VPN Concentrator or authentication server holds the rights for privileged administrators. The administrator is the only account that can edit the privileged administrators' rights. These rights control the configuration details that are available to a privileged administrator. For each configuration item the administrator can set the rights, read, change, denied, for each privileged administrator.

The VPN concentrator restricts the ability to generate RSA keys and install certificates to privileged administrators. . The VPN concentrator denies access to the DES, AES and HMAC keys except for the purposes of encryption. The VPN Client Keys are stored by the Operating System hosting the VPN Client during use.

If the VPN concentrator is to be managed remotely, the TOE requires administrators to first authenticate via IPsec.Auth (section 6.1.1.1).

6.1.3.2 Mgt.Client (VPN Client Configuration and Operation)

The Mgt.Client function associates the authentication credentials of the VPN Client with the TOE VPN Concentrator(s) that will authenticate the VPN Client and provide access to the correct trusted network.

This TSF requires a group name and group password or digital certificate to be defined to the VPN Client to identify the associated VPN Concentrator group (as described in section 6.1.3.4, Mgt.User). The VPN Client may also prompt for a

username and user password, if required by the VPN Concentrator, to identify the VPN Concentrator user (also described in section 6.1.3.4, Mgt.User).

If digital certificates are used, they must be installed on the VPN Client system using the Mgt.CertMgt TSF (section 6.1.3.5).

By default, the Hardware VPN Client will not allow incoming connections to the untrusted interface. Any packets received on the external interface that are not part of a valid VPN Tunnel will be dropped. The optional remote management function of the Hardware VPN Clients is not included in the evaluation.

6.1.3.3 Mgt.AuthServ (Authentication Server Configuration and Operation)

The TOE Authentication Server requires that administrators identify and authenticate themselves prior to allowing access to the Mgt.User (section 6.1.3.4) configuration attributes. Administrator accounts require a user name and password combination that matches a combination stored on the Authentication Server.

6.1.3.4 Mgt.User (Management of Groups and Users)

The TOE configuration data used to authenticate VPN Clients and enforce access controls is managed in terms of “groups” and “users”. Users are members of groups, and groups are members of the “base group”. Groups and users are identified by “group names” and “usernames” respectively, and have attributes that are configured via parameters. Attributes include passwords, filters, and whether split tunnelling is permitted.

Attributes are implemented hierarchically. When the VPN Concentrator checks parameters for a given VPN Client, the parameters used are extracted from attributes in the following order:

1. User attributes, which take precedence over any others,
2. Group attributes for the IPSec Tunnel Group, for any attributes not provided by the user attributes, and
3. Base Group attributes, for any remaining attributes.

Users and Groups, and their associated attribute parameters can be configured and stored on the TOE VPN Concentrator or on the TOE Authentication Server. When stored on the Authentication Server, attributes and their associated parameters are retrieved from the Authentication Server by the VPN Concentrator using the RADIUS authentication protocol. The VPN Concentrator and Authentication Server authenticate each other using a shared secret key.

6.1.3.5 Mgt.CertMgt (Digital Certificate Management)

The VPN Software Client, VPN Hardware Clients (PIX 501, Cisco 831 and 837, VPN 3002 and 3002-8E) and VPN Concentrator generate RSA public/private keys of length 512, 768, 1024 and 2048 bits, 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. Only an authorised administrator of the VPN Concentrator can initiate a SCEP request on the VPN Concentrator. SCEP is defined in Cisco System's Simple Certificate Enrollment Protocol White Paper².

6.1.3.6 Mgt.EventLog (Logging of Events)

The TOE VPN Concentrator generates system messages that identify specific TOE operations. System messages can be directed to an internal event log, which can be browsed by authorised users, or an external system outside of the TOE using the SYSLOG or SMTP (email) protocols. The VPN concentrator will generate audit messages for the events listed in section 5.2.1.

6.1.3.7 Mgt.Clock (Maintenance of Time)

The TOE VPN Concentrator provides a source of date and time for the TOE. The TOE VPN Concentrator will maintain time using a hardware clock, which will maintain time even if mains power is removed.

² Cisco System's Simple Certificate Enrollment Protocol White Paper, Copyright © 1998. Available from http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.pdf

7 Rationales

The purpose of this 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.

7.1 Security Objectives Rationale

	O.UserAuth	O.Secure	O.EAL	O.ConfigAccess	O.Roles	O.PacketFilter	O.SplitControl	O.Audit	O.ClientControls	OE.UserAuth	OE.Users	OE.Administrators	OE.ClientOS	OE.Certificates	OE.Token
T.Snoop		✓	✓					✓				✓		✓	✓
T.Configuration	✓		✓	✓	✓	✓		✓				✓			
T.Authenticate		✓	✓					✓		✓	✓	✓	✓	✓	✓
T.Insert		✓	✓					✓							
T.Modify		✓	✓					✓							
T.SplitTunnel			✓			✓	✓	✓				✓			
T.UserAccess			✓					✓	✓						

Table 7-1 - Mapping of Threats to Objectives

	OE. UserAuth	OE. Users	OE. Administrators	OE. ClientOS	OE. Certificates	OE. Token
A. Network			✓			
A. Admin			✓			
A. Users		✓				
A. Passwords			✓			
A. OS				✓		
A. Con-Physical			✓			
A. LAN-Physical			✓			
A. Soft-Secure			✓	✓		✓
A. Token	✓				✓	✓
A. Certificates					✓	✓
A. Remote			✓			

Table 7-2 - Mapping of Assumptions to Environmental Security Objectives

Threat	Objectives
T.Snoop	<p>O.Secure is suitable to counter to this threat as all traffic between the TOE VPN Client and TOE VPN concentrator will be securely encrypted preventing attackers from being able to obtain data from transmissions.</p> <p>Additionally, the environment provides counters to this threat by ensuring that OE.Certificate and OE.Token provides secure certificate services and storage to ensure that certificates used for encryption are not compromised when using a token in conjunction with the Windows VPN Client.</p>
T.Configuration	<p>O.UserAuth, O.ConfigAccess and O.Roles combine to counter this threat. O.ConfigAccess ensures that only Administrators can change the configuration of the TOE. O.UserAuth supports O.ConfigAccess by requiring that all interaction with the TOE is conducted by authorised “Users”. O.Roles ensures that not all authenticated users can alter the configuration of the TOE by providing three types of users, namely Administrators, Privileged administrators and Users.</p> <p>Additionally, in the case of remote administration, the environment (OE.Administrators) supports by ensuring that all administration is conducted over an encrypted link, provided by the objective O.Secure. O.PacketFilter prevents access to the VPN concentrator from the untrusted network by users who are not authenticated.</p>
T.Authenticate	<p>O.Secure is suitable to counter this threat by ensuring that authentication credentials are not transmitted “in the clear” over the untrusted network.</p> <p>Additionally, the environment provides counters to this threat by ensuring that administrators and users comply with password policies (OE.Admin and OE.Users). OE.Administrators ensures that passwords are of appropriate complexity and length such that guessing them is unfeasible. OE.ClientOS ensures that the operating systems running the VPN Clients do not allow access to the authentication credentials to attackers or other users of the Trusted IT System. Finally, OE.Certificate provides secure certificate services and storage to ensure that certificates used for authentication are not compromised. OE.Token provides secure certificate services and storage to ensure that certificates used for authentication are not compromised when using a token in conjunction with the Windows VPN Client.</p> <p>When using a smart card Token with the Microsoft Windows client as an option, OE.UserAuth ensures that the card enforces authentication of the user, prior to making any of the</p>

Threat	Objectives
	services provided by the card available to the TOE.
T.Insert	O.Secure is suitable to counter this threat as any packets inserted into the encrypted and signed traffic, would be dropped as the signature for the packet would not be able to be verified by the receiving TOE.
T.Modify	O.Secure is suitable to counter this threat as any packets that are modified in the signed traffic, would be dropped as the signature for the packet would not be able to be verified by the receiving TOE.
T.SplitTunnel	O.PacketFilter and O.SplitTunnel are suitable to counter this threat by enabling the TOE to filter packets on the VPN Client interface when a secure tunnel has been established to the VPN Concentrator. The objective OE.Configuration supports this objective by ensuring that the VPN Clients are configured to only permit connections to authorised networks when a connection to the VPN concentrator is active.
T.User Access	The objective O.ClientControls is suitable to counter this threat by enabling the TOE to filter packets on both the internal and external interfaces. This will, intern, allow the restriction of access to internal network resources.
	<p>The objectives O.Audit and O.EAL assist the counter of all above threats.</p> <p>O.Audit provides tracking of the use of the TOE. The audit will allow administrators to monitor the TOE and take appropriate action should a potential breach be detected.</p> <p>O.EAL ensures that the TOE can be trusted to perform as specified in this ST. This ensures that the TOE will be resistant to the likely attackers.</p>

Table 7-3 - Security Objectives Rationale

Assumption	Objectives
A.Network	OE.Administrators completely upholds this assumption, as the administrators will follow network security Policies, protecting the network to the appropriate level.
A.Admin	OE.Administrators completely upholds this assumption as the administrators are trained in the secure usage and configuration of the TOE and trusted to follow the supplied guidance.
A.Users	OE.Users completely upholds this assumption as the users are trained in the secure usage of the TOE and trusted to follow the supplied guidance.
A.Passwords	OE.Administrators completely upholds this assumption, as the administrators will follow network security Policies, including setting appropriate passwords for users.
A.OS	OE.ClientOS fully upholds this assumption as the Operating systems are configured in a secure manner and have all appropriate patches applied.
A.Con-Physical	OE.Administrators completely upholds this assumption as administrators are trained and will protect the TOE from physical attacks.
A.LAN-Physical	OE.Administrators completely upholds this assumption as administrators are trained and will protect the trusted LAN's from physical or logical attacks.
A.Soft-Secure	OE.Users and OE.Administrators completely upholds this assumption as users are trained and will protect the trusted IT system from physical attacks.
A.Token	OE.UserAuth, OE.Certificates and OE.Token completely uphold this assumption as the use of trusted tokens is an integral component of a trusted certificate management process.
A.Certificates	OE.Certificates completely upholds this assumption as the trusted certificate management process will result in trusted CAs being used to generate authentication certificates.
A.Remote	OE.Administrators completely upholds this assumption as administrators are trained and will configure the TOE to only use the encrypted links if managing the TOE across the untrusted network.

Table 7-4 - Environmental Objectives Rationale

7.2 Requirements Rationales

	O.UserAuth	O.Secure	O.ConfigAccess	O.Roles	O.PacketFilter	O.SplitControl	O.Audit	O.ClientControls	O.EAL	OE.UserAuth	OE.Users	OE.Administrators	OE.ClientOS	OE.Certificates	OE.Token
FAU_AUD.1							✓								
FAU_SAR.1							✓								
FCS_CKM.1/RSA	✓														
FCS_CKM.1/DES		✓													
FCS_CKM.1/AES		✓													
FCS_CKM.1/HMAC		✓													
FCS_CKM.4		✓													
FCS_COP.1/Encryption		✓													
FCS_COP.1/Signing	✓	✓													
FCS_COP.1/Auth	✓														
FDP_ACC.2		✓	✓												
FDP_ACF.1		✓	✓												
FDP_IFC.2					✓	✓		✓							
FDP_IFF.1					✓	✓		✓							
FDP_UCT.1		✓													
FDP_UIT.1		✓													
FIA_ATD.1/Users	✓			✓											
FIA_ATD.1/Admin	✓			✓											
FIA_UAU.2	✓														
FIA_UAU.5	✓														
FIA_UID.2	✓														
FMT_MOF.1			✓												
FMT_MSA.1/Conf			✓												
FMT_MSA.1/Keys	✓	✓													
FMT_MSA.2	✓	✓													

	O.UserAuth	O.Secure	O.ConfigAccess	O.Roles	O.PacketFilter	O.SplitControl	O.Audit	O.ClientControls	O.EAL	OE.UserAuth	OE.Users	OE.Administrators	OE.ClientOS	OE.Certificates	OE.Token
FMT_MSA.3			✓												
FMT_SMR.1				✓											
FMT_SMR.3				✓											
FPT_STM.1							✓								
FTA_TSE.1					✓										
FTP_ITC.1/Client		✓													
FTP_ITC.1/AuthSvr	✓														
SAR (EAL2 package)									✓						
FCS_CKM.1/TOK_RSA														✓	✓
FCS_CKM.4/TOK														✓	✓
FCS_COP.1/TOK_Auth														✓	✓
FIA_UAU.2/TOK										✓					✓
FIA_UID.2/TOK										✓					✓
FMT_MSA.1/TOK_Keys														✓	
FMT_MSA.2/TOK										✓					✓

Table 7-5 - Mapping of Objectives to Security Requirements

Objectives	Requirements
O.UserAuth	<p>O.UserAuth is provided in part by the SFRs FIA_UAU.2, FIA_UAU.5, FIA_UID.2 and FTP_ITC.1/AuthSvr. These SFRs require that the users and administrators are identified (FIA_UID.2) and authenticated (FIA_UAU.1) before any interaction with the TSFs. The SFR FIA_UAU.5 provides different authentication methods. The SFR FTP_ITC.1/AuthSvr provides a trusted path between the Authentication server and the VPN Concentrator, should centralised authentication be required.</p> <p>FCS_COP.1/Auth ensures that the certificates are valid, by verifying the RSA signature of the remote certificate using the public key of the trusted CA. SCEP is implemented by FCS_COP.1/Auth and FCS_COP.1/Signing. SCEP provides a secure method for installing certificates into the TOE. FCS_CKM.1/RSA provides valid keys to perform authentication between the VPN Client and the VPN Concentrator. FMT_MSA.1/Keys ensures that keys are stored correctly in the VPN Concentrator and Hardware VPN Client, and FMT_MSA.2 ensures that keys used for authentication are secure. Keys on the Software VPN Clients are protected by the host operating system.</p> <p>The SFRs FIA_ATD.1/Users and FIA_ATD.1/Admin provide for the storage of the authentication credentials for both administrators and users.</p> <p>Given that users are identified and authenticated, and that the authentication details can be associated to users of the TOE, this objective is met by the Security Functional Requirements of the TOE.</p>
O.Secure	<p>The primary aim of this objective is to provide secure encryption services. To provide secure encryption, Key management and trusted channels must be provided.</p> <p>Encryption is provided by the following SFRs which actually provide the requirements for the cryptographic operations, FCS_COP.1/Encryption, and FCS_COP.1/Signing</p> <p>FCS_COP.1/Encryption provides bulk encryption services ensuring that the traffic is kept obscured. FCS_COP.1/Signing provides signing services ensuring that that the traffic has not been modified in transit and that origin is known. The following SFRs, FDP_UCT.1 and FDP_UTI.1 ensure that the traffic transmitted between the VPN concentrator and the VPN Clients are protected from disclosure, modification, insertion and replay.</p> <p>Key generation is provided by FCS_CKM.1/DES and</p>

Objectives	Requirements
	<p>FCS_CKM.1/AES which provides means for the VPN Client and VPN concentrator to generate a common bulk encryption key. Additionally the generation of keys HMAC keys is provided by FCS_CKM.1/HMAC, which are required for signed messages. FCS_CKM.4 ensures that all encryption and signing key material is disposed of securely.</p> <p>FMT_MSA.1/Keys ensures that all encryption and signing key material is generated by the TOE. FMT_MSA.2 ensures that the values used for the keys are secure. FDP_ACC.2 and FDP_ACF.1 ensure that encryption and signing keys are only accessible by the TOE.</p> <p>Trusted channels are provided by FTP_ITC.1/Client through encryption.</p>
O.ConfigAccess	<p>FDP_ACF.1 and FDP_ACC.2 provide the policy and enforcement of the policy that will restrict access to the configuration data to privileged administrators.</p> <p>FMT_MSA.1/Conf and FMT_MSA.3 together provide the definition for which roles can alter which data, and ensure that by default the configuration of the TOE is restrictive. .</p> <p>FMT_MOF.1 further supports the above SFRs by restricting the ability to change the functions that implement the control of the configuration to privileged administrators.</p> <p>As access to the configuration is restricted, the SFRs will support the Objective O.ConfigAccess.</p>
O.Roles	<p>FMT_SMR.1, FIA_ATD.1/Users and FIA_ATD.1/Admin provide the ability to associate user with roles. FMT_SMR.3 requires that users make an explicit request to assume the roles. This meets the objective that users are associated with roles.</p>
O.PacketFilter	<p>FDP_IFC.2 and FDP_IFF.1 provide the policy and enforcement of the policy that will restrict access to the connectivity functions, and hence access to encryption functionality and the internal network, to authorised users.</p> <p>FTA_TSE.1 supports this functionality by allowing the TOE to deny specified IP Addresses.</p>
O.SplitControl	<p>FDP_IFC.2 and FDP_IFF.1 provide the policy and enforcement of the policy that will provide protection to the VPN Client by restricting access to the VPN Client host when a VPN session is active.</p>
O.Audit	<p>FAU_AUD.1 and FAU_SAR.1 are sufficient to meet the objective as they provide capability to generate, and read audit records. FPT_STM.1 provides the reliable time required for the audit records.</p>

Objectives	Requirements
O.ClientControls	FDP_IFC.2 and FDP_IFF.1 are sufficient to meet this objective as they provide the capability to restrict information flow control as defined in the information flow control SFP.
O.EAL	The SARs contained in the EAL2 package provide low to medium assurance and has been shown to have no obvious vulnerabilities.
OE.UserAuth	<p>When the option of using a token is employed with the Windows VPN Client, OE.UserAuth is provided in part by FIA_UAU.2/TOK, FIA_UID.2/TOK and FMT_MSA.2/TOK. These SFRs require that the users are identified (FIA_UID.2/TOK) and authenticated (FIA_UAU.2/TOK) before any interaction with the TSFs is permitted.</p> <p>FMT_MSA.2/TOK ensures that keys used for authentication are secure. Keys on the tokens are protected by the token operating system.</p>
OE.Users	Satisfied by A.Users.
OE.Administrators	Satisfied by A.Admin and A.Passwords.
OE.ClientOS	Satisfied by A.OS.
OE.Certificates	<p>When the option of using a token is employed with the Windows VPN Client, OE.Certificates is provided in part by FCS_CKM.1/TOK_RSA, FCS_CKM.4/TOK and FCS_COP.1/TOK_Auth. FCS_CKM.1/TOK_RSA provides valid keys to perform authentication between the VPN Client and the VPN Concentrator. FCS_CKM.4/TOK ensures that all signing key material held by the token is disposed of securely. FCS_COP.1/TOK_Auth provides signing services ensuring that that the traffic has not been modified in transit and that origin is known. FMT_MSA.1/TOK_Keys ensures that the values used for the keys are secure.</p>
OE.Token	<p>When the option of using a token is employed with the Windows VPN Client, OE.Token is provided in part by FCS_CKM.1/TOK_RSA, FCS_CKM.4/TOK and FCS_COP.1/TOK_Auth. FCS_CKM.1/TOK_RSA provides valid keys to perform authentication between the VPN Client and the VPN Concentrator. FCS_CKM.4/TOK ensures that all signing key material held by the token is disposed of securely. FCS_COP.1/TOK_Auth provides signing services ensuring that that the traffic has not been modified in transit and that origin is known. FMT_MSA.2/TOK ensures that all signing key material is generated by the Token.</p>

Table 7-6 - Requirements Rationale

7.3 TOE Summary Specification Rationales

	IPSec.Auth	IPSec.Encrypt	Filtering.Interface	Filtering.Client	Filtering.SplitControl	Mgt.User	Mgt.Conc	Mgt.Client	Mgt.AuthServ	Mgt.EventLog	Mgt.Clock	Mgt.CertMgt
FAU_AUD.1										✓		
FAU_SAR.1										✓		
FCS_CKM.1/RSA												✓
FCS_CKM.1/DES	✓											
FCS_CKM.1/AES	✓											
FCS_CKM.1/HMAC	✓											
FCS_CKM.4	✓	✓										
FCS_COP.1/Encryption		✓										
FCS_COP.1/Signing		✓										✓
FCS_COP.1/Auth	✓											✓
FDP_ACC.2							✓		✓			
FDP_ACF.1							✓		✓			
FDP_IFC.2	✓		✓	✓	✓		✓					
FDP_IFF.1	✓		✓	✓	✓		✓					
FDP_UCT.1		✓										
FDP_UIT.1		✓										
FIA_ATD.1/Users						✓	✓		✓			
FIA_ATD.1/Admin							✓		✓			
FIA_UAU.2	✓						✓		✓			
FIA_UAU.5	✓						✓		✓			
FIA_UID.2	✓						✓		✓			
FMT_MOF.1			✓				✓	✓	✓			
FMT_MSA.1/Conf			✓				✓	✓	✓			
FMT_MSA.1/Keys	✓						✓		✓			

	IPSec.Auth	IPSec.Encrypt	Filtering.Interface	Filtering.Client	Filtering.SplitControl	Mgt.User	Mgt.Conc	Mgt.Client	Mgt.AuthServ	Mgt.EventLog	Mgt.Clock	Mgt.CertMgt
FMT_MSA.2	✓											✓
FMT_MSA.3	✓						✓					
FMT_SMR.1						✓	✓		✓			
FMT_SMR.3						✓	✓		✓			
FPT_STM.1											✓	
FTA_TSE.1			✓		✓							
FTP_ITC.1/Client	✓	✓										
FTP_ITC.1/AuthSvr						✓						

Table 7-7 - Mapping of Functional Requirements to TOE Security Functions

Requirement	TSFs
FAU_AUD.1	The requirement FAU_AUD.1 is fully implemented by the TSF Mgt.EventLog, as the TSF is responsible for generating audit records and sending them to the configured log.
FAU_SAR.1	The requirement FAU_SAR.1 is fully implemented by the TSF Mgt.EventLog. The TSF provides the privileged administrators the capability to read the audit records that are stored in the TOE internal log.
FCS_CKM.1/RSA	The requirement FCS_CKM.1/RSA is fully implemented by the TSF Mgt.CertMgt. The TSF provides the capability to generate RSA keys. This capability is used when obtaining certificates for Authentication.
FCS_CKM.1/DES	The requirement FCS_CKM.1/DES is fully implemented by the TSF IPsec.Auth. The TSF generates 3DES and AES keys using Diffie-Hellman as part of the IKE authentication process.
FCS_CKM.1/AES	The requirement FCS_CKM.1/AES is fully implemented by the TSF IPsec.Auth. The TSF generates AES keys using Diffie-Hellman as part of the IKE authentication process.
FCS_CKM.1/HMAC	The requirement FCS_CKM.1/HMAC is fully implemented by the TSF IPsec.Auth. The TSF generates HMAC keys as part of the IKE authentication process.
FCS_CKM.4	The requirement FCS_CKM.4 is fully implemented by the TSFs IPsec.Auth, and IPsec.Encrypt. IPsec.Auth and IPsec.Encrypt overwrite obsolete DES, AES and HMAC keys and seeds with a sequence of bits.
FCS_COP.1/Encryption	The requirement FCS_COP.1/Encryption is fully implemented by the TSF IPsec.Encrypt. The TSF implements 3DES and AES encryption as part of the IPsec encryption process.
FCS_COP.1/Signing	The requirement FCS_COP.1/Signing is fully implemented by the TSFs IPsec.Encrypt and Mgt.CertMgt. The TSF IPsec.Encrypt implements HMAC in conjunction with MD-5 or SHA-1 to provide secure signing services as part of the IPsec encryption process. Mgt.CertMgt implements the MD-5 algorithm to produce the Thumbprint required for verifying the CA certificate (as part of SCEP).
FCS_COP.1/Auth	The requirement FCS_COP.1/Auth is fully implemented by the TSFs IPsec.Auth and Mgt.CertMgt. The TSF implements the verification of certificates using the RSA keys provided in the certificate. The certificate is verified against the trusted CA certificate to ensure that the remote instance of the TOE (be it VPN Concentrator or VPN Client) is valid. TSF

Requirement	TSFs
	Mgt.CertMgt implements the client (i.e. CA Client) side of SCEP, i.e. the VPN concentrator can communicate with a trusted CA to obtain a certificate securely using the SCEP protocol. SCEP implements client side RSA signature generation and verification. The VPN Client certificate is obtained through a trusted process (A.Certificates).
FDP_ACC.2	The requirement FDP_ACC.2 is fully implemented by the TSFs Mgt.Conc and Mgt.AuthServ. Mgt.Conc requires administrators identify and authenticate themselves before allowing access to configuration attributes. Mgt.AuthServ requires administrators to identify and authenticate themselves before accessing configuration attributes on the authentication server.
FDP_ACF.1	The requirement FDP_ACF.1 is fully implemented by the TSFs Mgt.Conc and Mgt.AuthSvr. Mgt.Conc allows only administrators and privileged administrators to access to the VPN concentrator configuration data as permitted by their configured rights. Mgt.AuthSvr allows only administrators of the Authentication Server to edit user data.
FDP_IFC.2	<p>The requirement FDP_IFC.2 is implemented by IPsec.Auth, Filtering.Interface, Filtering.Client, Filtering.SplitControl and Mgt.Conc. IPsec.Auth provides the capability to identify and authenticate users through the IKE process. This process requires that the VPN Client authenticate itself with either a certificate or group names/passwords and/or User names/passwords. A connection is denied if the user cannot present authentication details. Filtering.Interface allows the administrator to set conditions that must be met for connections to be established. These parameters are listed in section 6.1.2.1. Filtering.SplitControl prevents VPN Clients from having a connection to an untrusted network and the VPN concentrator at the same time. This also prevents attackers on the untrusted network from using the VPN Client as a step into the trusted network. Mgt.Conc allows only privileged administrators access to the configuration functions and data.</p> <p>The TSF Filtering.Client provides the ability filter incoming VPN Client traffic to restrict access to internal network resources that are not permitted to access.</p>
FDP_IFF.1	The requirement FDP_IFF.1 is implemented by IPsec.Auth, Filtering.Interface, Filtering.Client, Filtering.SplitControl and Mgt.Conc. . IPsec.Auth provides the capability to identify and authenticate users through the IKE process. This process requires that the VPN Client authenticate itself with either a certificate or group names/passwords and/or User

Requirement	TSFs
	<p>names/passwords. A connection is denied if the user cannot present authentication details. Filtering.Interface allows the administrator to set conditions that must be met for connections to be established. These parameters are listed in section 6.1.2.1. Filtering.SplitControl prevents VPN Clients from having a connection to an untrusted network and the VPN concentrator at the same time. This also prevents attackers on the untrusted network from using the VPN Client as a step into the trusted network. Mgt.Conc allows only privileged administrators access to the configuration functions and data.</p> <p>The TSF Filtering.Client provides the ability filter incoming VPN Client traffic to restrict access to internal network resources that are not permitted to access.</p>
FDP_UTC.1	<p>The requirement FDP_UTC.1 is fully implemented by the TSF IPsec.Encrypt. The TSF IPsec.Encrypt provides the encryption and signing services, using the keys generated as part of the authentication phase. The encryption ensures that the communication between the VPN Concentrator and a specific VPN Client can only be received and understood by the sending and receiving TOE.</p>
FDP_UIT.1	<p>The requirement FDP_UIT.1 is fully implemented by the TSF IPsec.Encrypt. The TSF IPsec.Encrypt provides the encryption and signing services, using the keys generated as part of the authentication phase. The signing functionality based on the shared secret key ensures that the VPN Concentrator or VPN Client can be certain that the communication came from the other party holding the shared secret key.</p>
FIA_ATD.1/Users	<p>The requirement FIA_ATD.1/Users is fully implemented by the TSFs Mgt.User, Mgt.Conc and Mgt.AuthServ. The TSFs Mgt.User and Mgt.AuthServ provide the capability to maintain users and associate those users with their authentication credentials (including group attributes) and filters. The TSF Mgt.Conc allows administrators to create and maintain users and their associated access (filters). Filters can be applied at multiple levels (i.e. user and/or group) as specified in the TSF.</p>
FIA_ATD.1/Admin	<p>The requirement FIA_ATD.1/Admin is fully implemented by the TSF Mgt.Conc and Mgt.AuthServ. The TSFs Mgt.Conc and Mgt.AuthServ provide the capability to maintain administrators and associate those administrators with their authentication credentials and privileges.</p>
FIA_UAU.2	<p>The requirement FIA_UAU.2 is fully implemented by the</p>

Requirement	TSFs
	<p>TSFs IPSec.Auth, Mgt.Conc and Mgt.AuthServ. The TSF IPSec.Auth authenticates users as part of the IKE process. The user is required to either provide user/group names and passwords (shared secret authentication) or certificate (certificate authentication). Users cannot interact with the VPN concentrator until they are authenticated. The VPN Client will not commence encryption until the IKE process is successful. The TSFs Mgt.Conc and Mgt.AuthServ require that administrators are identified and authenticated by user names and passwords before any TSF configuration options are available.</p>
FIA_UAU.5	<p>The requirement FIA_UAU.5 is fully implemented by the TSFs IPSec.Auth, Mgt.Conc and Mgt.AuthServ. The TSF IPSec.Auth authenticates users as part of the IKE process. The user is required to either provide user/group names and passwords (shared secret authentication) or certificate (certificate authentication). Users cannot interact with the VPN concentrator until they are authenticated. The VPN Client will not commence encryption until the IKE process is successful. The TSFs Mgt.Conc and Mgt.AuthServ require that administrators are identified and authenticated by user names and passwords before any TSF configuration options are available.</p>
FIA_UID.2	<p>The requirement FIA_UID.2 is fully implemented by the TSFs IPSec.Auth, Mgt.Conc and Mgt.AuthServ. The TSF IPSec.Auth identifies users as part of the IKE process. The user is required to either provide user/group names and passwords (shared secret authentication) or certificate (certificate authentication). Users cannot interact with the VPN concentrator until they are identified and authenticated. The VPN Client will not commence encryption until the IKE process is successful. The TSFs Mgt.Conc and Mgt.AuthServ require that administrators are identified and authenticated by user names and passwords before any TSF configuration options are available.</p>
FMT_MOF.1	<p>The requirement FMT_MOF.1 is fully implemented by the TSF Mgt.Conc and Mgt.AuthServ. The TSFs Mgt.Conc and Mgt.AuthServ require that administrators are identified and authenticated by user names and passwords before any TSF configuration options are available. Filtering.Interface restricts the opportunity for the administrator to be attacked from the untrusted interface, as communication to that interface is required to be authenticated as user traffic. Mgt.ClientMgt restricts access to the Hardware VPN Clients so that they cannot be used by an attacker on the untrusted network.</p>

Requirement	TSFs
FMT_MSA.1/Conf	The requirement FMT_MSA.1/Conf is fully implemented by the TSF Mgt.Conc, Mgt.ClientMgt, Filtering.Interface and Mgt.AuthServ. The TSFs Mgt.Conc and Mgt.AuthServ require that administrators are identified and authenticated by user names and passwords before any TSF configuration options are available. Filtering.Interface restricts the opportunity for the administrator accounts to be attacked from the untrusted interface, as communication to that interface is required to be authenticated as user traffic. Mgt.ClientMgt restricts access to the Hardware VPN Clients so that they cannot be used by an attacker on the untrusted network.
FMT_MSA.1/Keys	The requirement FMT_MSA.1/Keys is fully implemented by the TSF IPsec.Auth, Mgt.Conc and Mgt.AuthServ. The TSF IPsec.Auth generates the keys for bulk encryption. No users or administrators provide this information. The TSFs Mgt.Conc and Mgt.AuthServ require that administrators are identified and authenticated by user names and passwords before any TSF configuration options are available. Only the privileged administrators can generate VPN Concentrator RSA keys.
FMT_MSA.2	The requirement FMT_MSA.2 is fully implemented by the TSFs IPsec.Auth and Mgt.CertMgt. These TSFs are responsible for the generation of encryption and signing keys, namely 3DES, AES and HMAC, and RSA respectively. Part of this responsibility is to ensure that the keys are secure values, i.e. of appropriate complexity.
FMT_MSA.3	The requirement FMT_MSA.3 is fully implemented by the TSF Mgt.Conc. This TSF implements this requirement by ensuring that only administrators can change the configuration of the VPN Concentrator. Additionally, the default (installation) values of the TOE are restrictive, as they do not allow any network access to the TOE.
FMT_SMR.1	The requirement FMT_SMR.1 is fully implemented by the TSF Mgt.User, Mgt.Conc and Mgt.AuthServ. The TSF Mgt.User and Mgt.AuthServ provide the ability for the TOE to maintain users and as such the user role. Mgt.Conc and Mgt.AuthServ provide the ability to maintain administrative users and as such the administration roles. The user accounts and administrator accounts are exclusive, i.e. an account cannot have both user and administrator rights.
FMT_SMR.3	The requirement FMT_SMR.3 is fully implemented by the TSF Mgt.User, Mgt.Conc and Mgt.AuthServ. The TSF Mgt.User and Mgt.AuthServ provide the ability for the TOE to maintain users and as such the user role. Mgt.Conc and

Requirement	TSFs
	Mgt.AuthSvr provide the ability to maintain administrative users and as such the administration roles. The user accounts and administrator accounts are exclusive, i.e. an account cannot have both user and administrator rights. Therefore, an explicit request is required to assume a role, if user rights are required a user account must be logged on, for administrator rights an administrator account must be logged on.
FPT_STM.1	The requirement FPT_STM.1 is fully implemented by the TSF Mgt.Clock, which provides a hardware clock usable by any other functions of the TOE.
FTA_TSE.1	The requirement FTA_TSE.1 is fully implemented by the TSFs Filtering.Interface, and Filtering.SplitControl. The TSF Filtering.Interface will filter traffic, i.e. prevent traffic from passing, to the VPN Concentrator interface based on the configuration options set by the administrator. These configurable options are IP Address, port and IP protocol. The TSF Filtering.SplitControl ensures that traffic from the VPN Client is from the VPN Client and not traffic from an attacker on an untrusted network that is using the VPN Client as an access point.
FTP_ITC.1/Client	The requirement FDP_ITC.1 is fully implemented by the TSFs IPsec.Auth and IPsec.Encrypt. The TSF IPsec.Auth ensures that the VPN Concentrator verifies the identity of remote VPN Clients as part of IKE, either through certificates or user and group names and passwords. During the authentication process shared secret keys are generated, using Diffie-Hellman and HMAC key generation, ensuring that only the VPN Concentrator and VPN Client have the encryption and signing keys. The TSF IPsec.Auth provides the encryption and signing services, using the keys generated as part of the authentication phase. The encryption ensures that the communication between the VPN Concentrator and a specific VPN Client can only be understood by the holders of the secret keys. The signing functionality based on the shared secret keys ensures that the VPN Concentrator or VPN Client can be certain that the communication came from the other party holding the shared secret key.
FTP_ITC.1/AuthSvr	This SFR is fully implemented by the TST Mgt.User. Mgt.User provides functionality for the VPN Concentrator to communicate with the Authentication Server. These parts of the TOE communicate using TACACS+ and RADIUS, using a shared secret key for authentication.

Table 7-8 - TOE Summary Specification Rationale

7.4 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 of the Security Functions of the TOE are as follows:

- User Guidance (UG) Documentation;
- Design Specification (DS) Documents;
- Configuration Management Procedures (CMP) Document;
- Analysis of Testing (ATE) Document;
- Vulnerability Assessment (AVA) Document;

The assurance measures documents address the assurance requirements and are structured as follows:

7.4.1 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 the delivery procedures and how they maintain security during delivery to a user site (ADO_DEL.1)
- Describes procedures for the installation, generation, and start-up of the TOE (ADO_IGS.1)

7.4.2 Design Specification (DS) Documents

- Describes the security functionality of the TOE (ADV_FSP.1)
- Defines the external interfaces to the TOE (ADV_FSP.1)
- Defines the TOE in terms of sub-systems (ADV_HLD.1)
- Describes the relationship between TOE sub-systems (ADV_HLD.1)
- Identifies the sub-system interfaces and identifies the external interfaces (ADV_HLD.1)
- Demonstrates correspondence of the ST with the DS (ADV_RCR.1)

7.4.3 Configuration Management Procedures (CMP)

- Description of TOE Configuration Items, and identification of those items (ACM_CAP.2)

7.4.4 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)

7.4.5 Vulnerability Assessment (VA)

- Strength of TOE security function evaluation (AVA_SOF.1)
- Identifies obvious 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).

7.5 Security Assurance Requirements Rationale.

The developers have chosen EAL 2 because it provides a low to moderate level of independently assured security and ensures the TOE is structurally tested. EAL 2 requires the high-level design is independently analysed to provide assurance in the security functions of the token. The developers have determined this level of design information is suitable, sufficient and attainable. EAL 2 also requires independent testing, confirmation of developer testing, strength of function analysis and evidence of a developer search for obvious vulnerabilities. This testing and analyses is sufficient for the TOE to be securely used in its intended environment. EAL2 is also consistent with the Objective O.EAL.

7.6 Functional Dependencies

The TOE does not include FAU_GEN.1 as is required by the requirement FAU_SAR.1. The requirement FAU_SAR.1 provides the ability to read audit records. The requirement FAU_GEN.1 would generally provide the audit records to read. In this instance the audit records are generated by the requirement FAU_AUD.1. Therefore the dependency is satisfied.

The SFRs FCS_CKM.1 and FCS_COP.1 have a dependency on FCS_CKM.4, i.e. if keys are generated and used they must be destroyed. In this TOE, the DES, AES and HMAC keys are destroyed by overwrite. However, in the case of RSA public private key pairs the TOE does not explicitly destroy the keys. The RSA key pair is used for Authentication only and as such, if it is discovered masquerading of a user would be possible. The environment provides appropriate certificate management procedures to revoke certificates, invalidating the private key. No data is stored encrypted with the RSA private key. Therefore once a key is revoked (via a certificate revocation) the key is no longer useful to an attacker. As such, FCS_CKM.4 is not required for the RSA keys in this Security Target as there is no lasting use for keys.

The SFR FMT_MSA.2 has a functional dependency on ADV_SPM.1, i.e. Informal TOE security policy model. As recommended by Annex H.2 of CC Part 2, the secure values, and the reason that the values are secure, for FMT_MSA.2 have been defined in the application note associated with that SFR. The annex goes on to state that if these requirements are met, the dependency on ADV_SPM.1 can be argued away. As the application note provides the secure values required by the dependency and, ADV_SPM.1 is not required at the EAL2 assurance level, ADV_SPM.1 has not been included in the evaluation assurance package for the VPN 3000.

7.7 Mutual Support

7.7.1 Mutual Support of SFRs

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. CC Part 2 defines 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.

7.7.1.1 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 authorised.

The management function FMT_MSA.1 and FMT_MOF.1 support all other SFRs by restricting the ability to change management functions to privileged administrators, 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.

7.7.1.2 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 SFRs 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 authorised.

FMT_MSA.1 supports all other SFRs by restricting the ability to change certain management functions to authorised 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.

7.7.1.3 Help prevent de-activation of other SFRs

The Access Control policy detailed in FDP_ACF.1 along with the primary SFRs identified in table 8-9, provide for rigorous control of allowed data flow, preventing unauthorised deactivation of SFRs.

FMT_MSA.1 supports all other SFRs by restricting the ability to change management functions to privileged administrators, 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.

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 authorised.

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

7.7.2 Mutual Support of TSFs

The key functions of the TOE are IPSec.Auth and IPSec.Encrypt. These functions provide the authenticity and confidentiality of user data transmitted over an untrusted network.

The TSF IPSec.Auth supports the function IPSec.Encrypt by requiring that users are identified and authenticated prior to IPSec.Encrypt being granted a tunnel and keys to perform the encryption required to protect user data.

The Interface TSFs provide protection to these functions, preventing bypass of the authentication function (IPSec.Auth). These TSFs allow an administrator to restrict the access to the interfaces of the VPN Concentrator (Filtering.Interface) to allow connections only to ports on the VPN concentrator that require authentication. The interfaces on VPN clients can be configured to restrict connections to the client to specific known addresses when an ESP tunnel is established (Filtering.SplitControl). Further, the protection to data is further strengthened as the VPN Concentrator can be configured to restrict access to IP Addresses and ports on the trusted network based on the source and destination IP address and port (Filtering.Client).

The management functions (Mgt.Conc, Mgt.Client, Mgt.AuthServ and Mgt.User) provide the interface to administrators to configure all aspects of the security functions. The management functions allow the configuration of users, their authentication mechanisms, and filtering rules including, permitted access through the VPN Concentrator, and permitted split tunnelling capabilities. The management functions also allow the administrator to restrict access to the TOE by configuring the filter interfaces. Additionally, these functions support the above functions by restricting the access to management data to administrators. The management

functions allow the import of the VPN certificate (Mgt.CertMgt), which is the basis for certificate authentication of Users.

The Audit functionality (Mgt.EventLog) allows administrators to review the security relevant events permitting the administrators to understand the attacks the VPN Concentrator has been subjected to. This supports the above functions by assisting the administrators in identifying any further filters they need to implement to protect the data. The time function (Mgt.Clock) supports this by providing reliable time stamps for use by the audit function.

7.8 Strength of Function Rationale

The minimum Strength of Function for the TOE is SOF-Basic.

The Security Functional Requirements FIA_UAU.1 and FIA_UAU.5 provide the basis for the password mechanism. Passwords are inherently probabilistic and as such require a strength of function claim. The strength of function of the password in the TOE is SOF-Basic. The strength of function claim is based on the correct administration of the TOE. The assumptions to support the SOF claim are A.Passwords and A.Admin. These assumptions ensure that the TOE is configured correctly and include passwords that are appropriately complex.

The TSFs IPsec.Auth, Mgt.Conf and Mgt.AuthSvr inherit the SOF claim above, as they implement the password requirements from the above SFRs.

The claim for SOF-Basic is appropriate for this TOE as it is sufficient to protect against an attacker with a low attack potential, i.e. Attackers with high resources, high skill and low motivation.

Additionally, it is consistent with the evaluation level of EAL 2 and the testing that is carried out for that level.