Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Virtual Private Network (VPN) Platform Security Target

Version 11.0 Final
April, 2009

Table of Contents

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

List of Tables

Introduction

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Adaptive Security Appliances (ASA) 5500 series with concentration on VPN functionality to include IPSec and SSL implementations. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

Security Target Introduction

This section presents security target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

a. A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (refer to the "Security Environment" section on page 14).

b. A set of security objectives and a set of security requirements to address the security problem (refer to the "Security Objectives" section on page 14 and the "Security Requirements" section on page 17).

c. The IT security functions provided by the TOE that meet the set of requirements (refer to the "TOE Summary Specification" section on page 33).

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 4.

ST and TOE Identification

This section provides information needed to identify and control this ST and its TOE. This ST targets Evaluation Assurance Level EAL4 augmented with ALC_FLR.1.

ST Title	Cisco Adaptive Security Appliances (ASA) 5505, 5510, 5520, 5540 and 5550 Virtual Private Network (VPN) Platform Security Target
ST Version	Version 11.0 Final
Publication Date	April, 2009
Vendor	Cisco Systems, Inc
ST Authors	Cisco Systems, Inc
TOE Identification	Cisco ASA 5505, 5510, 5520, 5540 and 5550 (Release 7.2(4)), Cisco VPN Client Release 5.0.03.0560
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Common Criteria Conformance Claim	The ST is compliant with the Common Criteria (CC) Version 2.3 and took into account all NIAP and CCIMB interpretations up to the kick-off date of February 23, 2006. This ST uses the CCEVS Precedents PD-0108 to correctly specify remote administration. The ST is EAL4, Part 2 extended, and Part 3 augmented with ALC_FLR.1.
Protection Profile Conformance	The TOE does not claim conformance to any Protection Profile.
Security Target Evaluation Status	Version 11.0 Final
Keywords	Virtual Private Network, IPSec, SSL

Security Target Overview

The TOE consists of hardware and software used to construct Virtual Private Networks (VPNs). The TOE is a purpose-built platform that may be used, with or independent of its firewall, intrusion prevention system, and network antivirus capabilities, as a dedicated-function VPN platform.

For VPN Services, the ASA 5500 Series provides a complete remote-access VPN solution that supports numerous connectivity options, including Cisco VPN Client for IP Security (IPSec), WebVPN, and network-aware site-to-site VPN connectivity. IPSec provides confidentiality, authenticity, and integrity for IP data transmitted between trusted (private) networks over untrusted (public) links or networks. WebVPN uses a Web browser and SSL encryption to secure connections between remote users and specific, supported internal protected resources.

References

The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, version 2.3, CCMB-2005-08-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, version 2.3, CCMB--2005-08-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, version 2.3, CCMB-2005-08-003
[CEM]	Common Methodology for Information Technology Security Evaluation—Evaluation Methodology, dated August 2005, version 2.3 CCMB-2005-08-004

Acronyms and Abbreviations

The following acronyms and abbreviations are used in this Security Target:

Table 1 Acronyms and Abbreviations

Acronym or Abbreviations	Definition
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
EAL	Evaluation Assurance Level
FSP	Functional Specification
HLD	High Level Design
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPS	Intrusion Prevention System
IPSec	IP Security
IT	Information Technology
LAN	Local Area Network
MAC	Message Authentication Code
OS	Operating System
PKI	Public Key Infrastructure
PSK	Pre-shared Keys
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
SA	Security Association
SAR	Security Assurance Requirement
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TLS	Transport Layer Security
TSP	TOE Security Policy
VPN	Virtual Private Network

TOE Description

This section provides an overview of the Cisco Adaptive Security Appliance (ASA) Version 7.2(4)18 (hereafter referred to as 7.2(4)) to assist potential users in determining whether the Cisco ASA 5500 Series meets their needs for VPN functionality. This section also defines the physical and logical boundaries; summarizes the security functions; and describes the evaluated configuration.

TOE Product Type

The ASA controls the flow of Internet Protocol (IP) traffic (datagrams) between network interfaces. The ASA provides firewall, Anti-X, and VPN capabilities. For this Security Target, the ASA is considered to be a dedicated-function VPN platform providing packet filtering functionality for self protection. The appliance is provided on a number of platforms. The ASA platforms included within the scope of this evaluation are the Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550. From hereon these platforms will be refereed to as the Target of Evaluation (TOE). The ASA supports three types of VPN access to include IPSec-based remote access requiring the Cisco VPN client, WebVPN requiring a web browser, and LAN-to-LAN IPSec VPN requiring two ASA appliances. The Cisco VPN Client is considered to be part of the TOE.

TOE Overview

The TOE is a purpose-built hardware device that uses an Intel processor in all models. The ASA runs the Cisco Adaptive Security Appliance Software “image”. The TOE provides a single point of defense as well as controlled and audited access to services between networks by permitting or denying the flow of information traversing the appliance.

Virtual Private Network Concept

The TOE controls the flow of IP traffic between network interfaces. The network interfaces are either “internal” or “external”. If an interface is identified as external than the network to which it attaches is classed as being outside of the TOE. If an interface is identified as an internal interface than the network to which it attaches is classed as being inside (or behind) the TOE. All networks inside (or behind) are protected by the TOE against those outside the TOE. A VPN is a secure connection between a user on the outside network communicating with the TOE (a VPN device) that in turn gives the user access to the inside network. The VPN connection is considered secure because the user is authenticated and the network traffic is protected from disclosure and modification through encryption. Once a VPN session is established, the TOE will decrypt incoming packets received from the user and encrypt outgoing packets directed to the user.

IPSec VPN is a deployment proven remote-access technology. Because IPSec can transparently support any IP application, users can work remotely (from the external network) as if they were physically in the office, attached to their office LAN (internal network). IPSec VPN connections require the Cisco VPN client software. For LAN-to-LAN IPSec. two ASAs are required.

Using only a web browser and it native SSL encryption, WebVPN provides remote access without the requirement of pre-installed VPN client software. WebVPN provides the flexibility to support secure access for users, regardless of the endpoint device they are establishing the connection from. WebVPN provides access to a broad range of web resources and both web-enabled and legacy applications from almost any computer that can reach HTTPS sites. WebVPN uses SSL and its successor, Transport Layer Security (TLS) to provide a secure connection.

TOE Physical Boundary

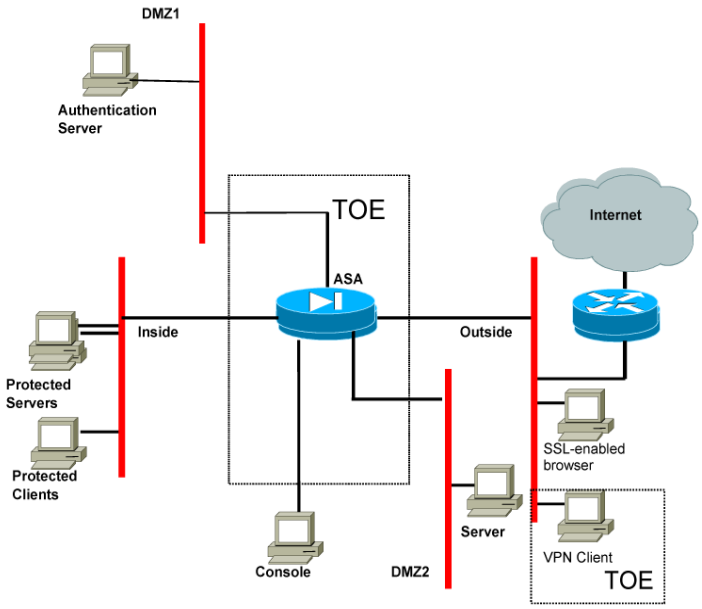
The TOE implements two types of physical configurations:

Remote access configurations – consisting of one ASA component which establishes and controls VPN connections and allows the flow of IP traffic between external and internal network interfaces, and a VPN Client Component executing on a physically secure, properly configured windows-based platforms.

LAN-to-LAN (Also referred to as Site-to-Site) configurations – consisting of a VPN tunnel between two ASA TOE instances connecting networks in different geographic locations.

Figure 1, depicts the TOE's physical boundary for remote access configurations. The VPN Client includes only the VPN client software, not the IT platform it runs on.

Figure 1 TOE Physical Boundary – Remote Access Configuration



The physical scope of the TOE includes the hardware and software elements identified in Table 2.

:

Table 2 TOE Component Identification

Hardware	Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 each with up to nine interfaces and the following processors: 5505- 500 MHz AMD GX3 5510 – 1.6 GHz Celeron 5520 – 2.0 GHz Celeron 5540 – 2.0 GHz Pentium 4 5550- 3.0 GHz Pentium 4
Software	Cisco Adaptive Security Appliance 'image' version 7.2(4) Cisco VPN Client Release 5.0.03.0560

The ASA 5500 series Adaptive Security Appliances only differ in hardware configuration and do not affect how the security functions specified in the ST are met. They are configurable with additional modules. The cryptographic accelerator is built-in to all of the appliances that are part of TOE. As well as the built-in network interfaces, the following network module is supported in this evaluation:

- 4-port 10/100/Gigabit Ethernet Module (part number ASA-SSM-4GE).

All ASA 5500 series Adaptive Security Appliances are available with either AC or DC power. As the power supplies do not provide any security enforcing functionality the AC and DC powered models are treated identically. The software executing on all the appliances is the same version of Cisco Adaptive Security Appliance “image’ version 7.2(4).

The TOE provides interconnections between two or more networks depending on the number of interface cards installed within the product. A combination of network cards can be installed in the Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550. The physical boundaries of the TOE are the physical port connections on the TOE external casing. One such port is to connect to the management console. Management of the TOE may be conducted either from a directly connected console (Illustrated in Figure 1), or from a network console linked via SSH. There are no constraints on the location of the network console. In both cases the console must be physically protected. The consoles are not part of the TOE.

A separate secure management network is used (see DMZ1 in Figure 1) for the Authentication Server. The TOE environment includes a commercially available TACACS+ or RADIUS Authentication Server. Users with VPN clients and SSL-capable web browsers are located on the outside network. A VPN Client Component is contained on a physically secure and properly configured IT system and connected to the untrusted network via some form of network interface, under the control of the host operating system, e.g. LAN. When active, the VPN Client Component provides confidentiality, authenticity, and integrity for traffic transmitted over the untrusted network to the ASA. The ASA interacts with one VPN Client component: the Cisco VPN Client (IPSec Client component). The Cisco VPN Client for Windows is software that runs on a physically secure and properly configured Windows-based PC and is used to create and maintain an IPSec-based VPN connection to the ASA. The Cisco VPN Client is part of the TOE.

TOE Logical Boundary

The TOE offers both IPSec and SSL-based VPN services on a single platform. For IPSec VPN, users (on the outside) can access virtually any application as if they were actually attached to the inside network. The IPSec service requires the Cisco VPN client executing on a physically secure and properly configured windows-based PC to establish an IPSec VPN connection. The TOE will authenticate the VPN client using pre-shared keys or digital certificates (RSA). If successful authentication is achieved, a secure channel is established by using triple DES and AES ciphers to provide confidentiality and MD5 and SHA-1 algorithms for integrity and authenticity protection.

The TOE provides one connectivity option for SSL-based VPN services: WebVPN. WebVPN requires an SSL-capable web browser to establish an SSL-based VPN connection. WebVPN will only allow the web browser to access web resources and web-enabled applications behind the TOE until after the user has been authenticated. Authentication is achieved by digital certificates, username/password, or validating an authentication cookie. The WebVPN implements the SSLv3 and TLS protocols with strengths up to 168 bit for Triple DES, and 128, 192, and 256 bit for AES. In general, the SSL protocol takes the application message (e.g., HTML) to be transmitted, fragments the data into manageable blocks, compresses the data, applies a message authentication code (MAC), encrypts, adds a header, and transmits the resulting unit as a TCP segment. Received data is decrypted, verified, decompressed, and reassembled and then delivered to the appropriate application.

An access control policy can be applied to VPN traffic, so individuals and groups of users have access to the applications, network services, and resources to which they are entitled. The TOE provides an authorized administrator the capability to define a single policy that incorporates both security and connectivity for remote users.

The TOE can be managed by authorized administrators via a physically secure local connection. The ASA appliance part of the TOE can also be managed remotely from a connected network, through SSH. The TOE supports the authentication of authorized administrators by means of user id and password, and, with support from the environment, supports the use of third party authentication servers.

The TOE provides audit generation and audit viewing capability via a configurable log file stored locally on the TOE.

The external authentication server used to provide authentication (if configured by the authorized administrator) is outside the scope of the TOE, although use made by the TOE of this server is within scope.

Non-Cisco clients such as an SSL-capable web browser used to establish a VPN session with the TOE is considered part of the TOE IT Environment.

TOE Features Excluded from Evaluation

The bulleted list below identifies functionality included in the TOE's physical boundary but not included in the TOE's logical boundary or claimed in the TOE's security functionality. The TOE features and hardware listed below are outside the scope of the defined TOE Security Functions (TSF) and are therefore not evaluated. The features listed below are non-interfering with the TSF.

- SSL VPN Client (SVC)
- Cut-through Proxies
- RIP
- SNMP
- DHCP Server
- Intrusion Prevention System capabilities
- TCP Port Forwarding
- Content filtering
- Anti-X capabilities
- CRACK authentication method
- Fail-over
- on the 5505: USB0, 1, and 2 ports
- on the 5510: USB1 and USB2 ports
- on the 5520: USB1 and USB2 ports
- on the 5540: USB1 and USB2 ports
- on the 5550: USB1 and USB2 ports

The following add-on modules were not evaluated and must be excluded from use in the TOE:

- AIP SSM (intrusion detection) and CSC SSM (Content Security) modules

TOE Security Architecture

The following sections provide details about how the security architecture of the TOE for this ST cannot be bypassed, corrupted, or otherwise compromised. An explanation is provided for how each TOE component supports the secure operation of the TSF and the role played by the IT environment is described.

ASA Appliance TOE Component

The ASA Appliance is a self contained hardware and software appliance. The ASA Appliance is used to construct Virtual Private Networks (VPNs) with remote users on an external network seeking to access resources on an internal network. The ASA Appliance is a dedicated device, with no general purpose operating system, disk storage, or programming interface. The ASA Appliance mediates the interfaces and communications and makes sure that the security enforcement functions are invoked and succeed before allowing any other mediated security function to be used. By doing this the ASA Appliance ensures that it and its security functions are non-bypassable.

The ASA Appliance maintains a security domain for its own use. The security domain is all the hardware and software that makes up the ASA Appliance. The ASA Appliance provides for isolation at the physical boundary of the component. For this reason the whole ASA Appliance is an isolated security domain. It separates itself from the external users and therefore helps in providing a tamper resistant domain that can not be interfered with. The ASA Appliance helps in keeping the domain separate and protected by controlling those interfaces into the component so that only trusted and authorized communications occur that are directly related to satisfying the ASA Appliance's capability to establish and control VPN sessions. The administrative interface is protected by authentication and by physical controls, and by means of encryption when used remotely. No untrusted processes are permitted on the ASA Appliance. Because the whole ASA Appliance is a separate physical domain and a dedicated platform solely supporting ASA processes and the fact that it controls and mediates access to its interfaces, it provides a security domain for the TSF that is protected from interference and tampering.

VPN Clients

The ASA interacts with a single VPN Client components: the Cisco VPN Client (IPSec Client component). The VPN Client components of the TOE are software applications that are resident on a physically secure and properly configured IT system within an associated host operating system. The IPSec Client component operates on a Microsoft Windows XP or Windows 2000 platform.

The IPSec Client component must be installed and configured with the authentication credentials and connection details necessary to authenticate the VPN Client to the ASA. Specific IPSec parameters and other configurations options for the IPSec Client component are downloaded from the ASA after successful authentication.

The VPN Client component intercepts all TCP/IP data between the physically secure and properly configured IT system (Windows OS) TCP/IP stack and network interfaces to determine whether the data must be encrypted/decrypted. The VPN Client component makes sure that VPN (IPSec) functions are invoked and succeed before allowing any other mediated action to occur. Through the mediation and control of the TCP/IP stack and VPN functions, the VPN Client component supports non-bypassability of its security functions. The IT environment of the VPN Client component supplies a physically secure and properly configured platform executing a Windows-based operating system to provide the execution environment for the VPN Client component. The IT environment is considered a physically secure and properly configured IT system that makes sure that all users are identified and authenticated into the IT Environment before they are allowed to carry out any other mediated action with the Windows OS and the resources that the Window OS controls. The Windows OS provides the control and mediation of

network interfaces to the platform hosting the VPN Client component. The ability of the Windows OS to mediate and control all its interfaces allows for the IT Environment to make sure that its enforcement functions are invoked and succeed before allowing any other mediated action with any of the other security functions hosted by the Windows OS. This provides for the non-bypassability of the IT Environment along with supporting the non-bypassability of the VPN Client component operating on the host platform composed of the Windows OS and its platform. The IT Environment is also assumed to be physically protected from unauthorized tampering. The non-bypassability features of the IT environment ensures that users are controlled and only use interfaces and have access to resources they are authorized for which helps in the non-bypassability of the VPN Client component by controlling and giving access to those interfaces that are within the control of the VPN Client component. The IT environment supplies process, memory, and address isolation for applications and system processes. Having process, memory, and address isolation allows for the Windows OS to establish a security domain for its security functions and allows for the Windows OS to provide separation between running processes. With these mechanisms and the hardware which is provided by the IT Environment domain separation is supported. Domain separation helps in the self protection of the VPN Client component. The Windows OS provides for the isolation of the VPN Client component from the other processes executing by providing a separated domains of execution.

Security Functions Claimed by the TOE

The TOE's security function (TSF) Functions summary and the identification of TOE data are described below.

TOE Data

Data in the TOE is categorized as either user data or TSF data. The following sections identify the data included in the TOE.

TSF Data

The TSF data for the TOE are the audit records, certificates, keys, user-oriented SSL attributes, user identity credentials, SSL configuration attributes, and IPSec configuration attributes.

User Data

The user data for the TOE is the network traffic information that is encrypted and decrypted for VPN connectivity.

Security Management

The TOE's security management functions provides security capabilities that guarantees all administrators are required to identify and authenticate to the TOE before any administrative or monitoring actions can be performed. The TOE only allows administration of the TOE to occur from the console port or from a network console via SSH. The TOE's Management Security Capability provides administrator support functionality that enables a human user to manage and configure the TOE.

Audit

The TOE's Audit security function supports audit record generation and review. The administrator can read audit records locally. The TOE provides date and time information that is used in audit timestamps.

IPSec VPN

The TOE implements the IETF IPSec protocols (RFCs 2401-2410) to provide confidentiality, authenticity, and integrity for packets flows transmitted from and received by the TOE.

SSL VPN

The TOE implements the SSLv3 and TLS protocol to provide SSL-based VPN connectivity.

Identification and Authentication

The TOE's Identification and Authentication security function provides I&A support of all client hosts (VPN Client Components and SSL-capable web browser) requesting a VPN session along with providing I&A support to make sure all administrator are properly identified and authenticated.

Self Protection

The ASA component provides for non-bypassability and domain separation of functions within the TOE's scope of control (TSC). To enable the TOE to be "self defending" the inbound filtering functions of the ASA are included. This allows (for example) IP packets that are not IPSec or SSL to be ignored by the TOE, which is particularly important as the TOE will typically operate with one interface facing a public network. The ASA controls actions carried out by a user by controlling a user's VPN session and the actions carried out during that session. By maintaining and controlling a VPN session a user has with the TOE, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE that prevents the TOE from being interfered or tampered with for those users that are within the TSC. Note that the VPN Client components rely on the IT environment to provide a protected security domain for execution and to help enforce non-bypassability protection.

Clock

The TOE uses an internal clock to provide a source of date and time information used to produced a reliable time stamp for audit record generation.

TOE Evaluated Configuration

The TOE's evaluated configuration requires one instance of an ASA appliance and one or more instances of a client host (VPN Client Components or SSL-capable web browser) for remote access configurations or two ASA appliances for LAN-to-LAN configurations. The TOE operates only in single-routed context mode. Multiple context mode is not supported in the evaluated configuration.

Additionally, the following list itemizes the evaluated configuration option requirements:

1. IPSec is enabled
2. SSL is enabled (WebVPN)

Note that the client host platform is not part of the TOE and is considered to be in the IT Environment.

The bulleted list below identifies features that must be disabled or otherwise inaccessible in the evaluated configuration.

- Telnet
- Transparent Mode

- Multi-context mode
- Auto sign-on (WebVPN)
- ASDM GUI
- SVC download

Security Environment

This section identifies the following:

a. Significant assumptions about the TOE's operational environment.

b. IT related threats to the organization countered by the TOE.

c. Environmental threats requiring controls to provide sufficient protection.

d. Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Policies are identified as P.policy with "policy" specifying a unique name.

Assumptions

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

Table 3 **TOE Assumptions**

Name	Assumption
A.No-Evil	As the security functions of the TOE can be compromised by an authorized administrator, administrators are assumed to be non-hostile and trusted to perform their duties correctly.
A.PhySec	As the security functions of the TOE can be compromised by an attacker with physical access to the TOE, it is assumed that the TOE is located in a physically secure environment.
A.Training	As the security functions of the TOE can be compromised due to errors or omissions in the administration of the security features of the TOE, it is assumed that administrators of the TOE have been trained to enable them to securely configure the TOE.
A.Trusted-CA	As the security functions of the TOE when configured to use digital certificates can be compromised if the Certificate Authority (CA) that issued the certificates is not operated in a trusted manner, it is assumed that if the TOE is configured to use digital certificates, the issuing CA is trusted to at least the same level as the TOE.
A.PSK	Pre-shared keys are assumed to be securely communicated between disparate administrators.
A.Host	The VPN Client Components will be installed on a physically protected, properly configured IT platform and operated in a secure manner.

Threats

Table 4 lists the threats addressed by the TOE and the IT Environment. For the threats below, attackers are assumed to be of low attack potential.

Table 4 Threats

Threat Name	Threat Definition
T.Attack	An attacker may gain access to the TOE and compromise its security functions by altering its configuration.
T.Untrusted-Path	An attacker may attempt to disclose, modify or insert data within packet flows transmitted/received by the TOE over an untrusted network. If such an attack was successful, then the confidentiality, integrity and authenticity of packet flows transmitted/received over an untrusted path would be compromised.
T.Audacc	Persons may not be accountable for the actions that they conduct because the audit records are not review, thus allowing an attacker to escape detection.
T.Lowexp	A skilled attacker with low attack potential may attempt to bypass the TSF to gain access to the TOE or the assets it protects.
T.No-Authentication	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE
T.Self-Protect	An unauthorized person may read, modify, or destroy security critical TOE configuration data.

Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.There are no organizational security policies for this TOE.

Security Objectives

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

- This document identifies objectives of the TOE as O.*objective* with *objective* specifying a unique name. Objectives that apply to the IT environment are designated as OE.*objective* with *objective* specifying a unique name.

Security Objectives for the TOE

Table 5 identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 5 Security Objectives for the TOE

Name	TOE Security Objective
O.Authenticity	The TOE must provide the means for ensuring that a packet flow has been received from a trusted source.
O.Audit-Record	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times.
O.Confidentiality	The TOE must protect the confidentiality of packet flows transmitted to/from the TOE over an untrusted network.
O.Integrity	The TOE must ensure that any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected.
O.ID-Authentication	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
O.Key-Confidentiality	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt packet flows between the TOE and a remote client and when kept in short and long-term storage.
O.No-Replay	The TOE must provide a means to detect that a packet flow transmitted to the TOE has not been copied by an eavesdropper and retransmitted to the TOE.
O.Secure-Operation	The TOE must prevent unauthorized changes to its configuration.
O.EAL	The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.
O.Self-Protect	The TOE must protect itself against attempts by unauthorized user to bypass, deactivate, or tamper with TOE security functions.

Security Objectives for the Environment

The assumptions identified in the "Assumptions" section on page 14 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 6 identifies the security objectives for the environment.

Table 6 Security Objectives for the Environment

Name	IT Environment Security Objective
OE.ID-Authentication	The claimed identity of a remote user must be uniquely identified and authenticated , before granting the user access to TOE functions or, for certain specified services, to a connected network.[1]
OE.Secure-Management	Those responsible for the operation of the TOE must ensure that the TOE environment is physically secure, and management and configuration of the security functions of the TOE are: **a.** initiated from a management station connected to a trusted network and protected using the security functions of the TOE, **b.** undertaken by trusted staff trained in the secure operation of the TOE, **c.** implemented in conjunction with an trusted Certificate Authority (CA), if digital certificates are used for TOE authentication, **d.** configured to interface only to trusted clock sources, and **e.** Pre-shared Keys used for configuration in cryptographic maps are securely distributed amongst disparate administrators.
OE.Client	Those responsible for the operation of the TOE must ensure the host platform and operating system that supports the VPN Client Components are physically protected, support the required SSL/TLS versions for correct SSL VPN implementation, and are securely configured and maintained to not negatively affect the correct operation of the TOE.

1. The objective ID-Authentication is present for both the TOE and the TOE environment. This reflects the use of an authentication server in the environment to generate authentication credentials where single-use authentication is applied for remote users.

Security Requirements

This section identifies the Security Functional Requirements for the TOE and for the IT Environment. The Security Functional Requirements included in this section are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* and all National Information Assurance Partnership (NIAP) and international interpretations up to the kick-off date of February 23, 2006, with the exception of the items listed below.

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC.

Assignments: indicated by showing the value in square brackets [Assignment_value].

Selections: indicated by italicized text.

Assignments within selections: indicated in italics and underlined text.

Refinements: indicated in **bold text** with the addition of details and ~~**bold text**~~ when details are deleted.

Multiple Security Functional Requirement instances (iterations) are identified by the Security Functional Requirement component identification followed by the instance number in parenthesis (e.g. FCO_NRO.2(1)) and the Security Functional Requirement element name followed by the instance number in parenthesis (e.g. FCO_NRO.2.1(1)). This document continues the iteration numbering for Security Functional Requirements that apply to both the TOE and the IT Environment.

Interpreted requirements are identified by appending "-NIAP" and interpretation number to the Security Functional Requirement component identification. Only the elements affected by the Interpretation are labelled by "-NIAP" and interpretation number to the Security Functional Requirement element.

Explicitly stated SFRs are identified by having a label (EXP) meaning 'Explicit Stated SFR for the TOE' after the requirement name for TOE SFRs.

TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in Table 7 are described in more detail in the following subsections.

Table 7 TOE Security Functional Requirements

Functional Component	Description
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FCO_NRO.2(1)	Enforced Proof of Origin – IPSec
FCO_NRO.2(2)	Enforced Proof of Origin – SSL
FCS_CKM.1(1)	Cryptographic Key Generation – RSA
FCS_CKM.1(2)	Cryptographic Key Generation – Diffie-Hellman
FCS_CKM.4(1)	Cryptographic Key Destruction
FCS_COP.1(1)	Cryptographic Operation – Encryption
FCS_COP.1(2)	Cryptographic Operation – Hashed Message Authentication Code Generation
FCS_COP.1(3)	Cryptographic Operation – Remote Administration
FCS_COP.1(4)	Cryptographic Operation – SCEP Signing
FCS_COP.1(5)	Cryptographic Operation – SCEP Encryption
FDP_IFC.1(1)	Subset Information Flow Control – IPSec
FDP_IFC.1(2)	Subset Information Flow Control – SSL
FDP_IFF.1(1)	Simple Security Attributes – IPSec
FDP_IFF.1(2)	Simple Security Attributes – SSL
FDP_UCT.1(1)	Basic Data Exchange Confidentiality – IPSec
FDP_UCT.1(2)	Basic Data Exchange Confidentiality – SSL
FDP_UIT.1(1)	Data Exchange Integrity – IPSec
FDP_UIT.1(2)	Data Exchange Integrity – SSL
FIA_UAU.2	User Authentication Before Any Action
FIA_UAU.5(1)	Multiple authentication mechanisms
FIA_UID.2(1)	User Identification Before Any Action
FMT_MOF.1(1)	Management of Security Functions Behavior
FMT_MOF.1(2)	Management of Security Functions Behavior
FMT_MSA.1(1)	Management of Security Attributes – IPSec
FMT_MSA.1(2)	Management of Security Attributes – SSL

Table 7 TOE Security Functional Requirements (continued)

Functional Component	Description
FMT_MSA.2(1)	Secure Security Attributes
FMT_MSA.3	Static Attribute Initialization
FMT_MTD.1(1)	Management of TSF Data
FMT_MTD.1(2)	Management of TSF Data
FMT_MTD.1(3)	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_AMT.1	Abstract Machine Testing
FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FPT_RVM.1(1)	Non-bypassability of the TSP
FPT_SEP.1(1)	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
FPT_TST.1	TSF Testing
FTA_TSE.1	TOE Session Establishment
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_RTC.1(EXP)	Remote Administration Trusted Channel

Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [errors during IPSec processing, errors during SSL processing, decisions on request for information flow, failures during digital certificate processing].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

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

FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] from the audit records.

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

Communication (FCO)

FCO_NRO.2(1) Enforced Proof of Origin - IPSec

FCO_NRO.2.1(1)	The TSF shall enforce the generation of evidence of origin for transmitted [IP packets protected by the IPSec information flow control SFP] at all times.
FCO_NRO.2.2 (1)	The TSF shall be able to relate the [IPSec SA peer] of the originator of the information, and the [digital signature] of the information to which the evidence applies.
FCO_NRO.2.3 (1)	The TSF shall provide a capability to verify the evidence of origin of information to *the receiving SA peer* given [the successful establishment of an IPSec SA with the transmitting SA peer].

FCO_NRO.2(2) Enforced Proof of Origin - SSL

FCO_NRO.2.1(2)	The TSF shall enforce the generation of evidence of origin for transmitted [HTTP packets protected by the SSL information flow control SFP] at all times.
FCO_NRO.2.2(2)	The TSF shall be able to relate the [SSL session] of the originator of the information, and the [digital signature] of the information to which the evidence applies.
FCO_NRO.2.3 (2)	The TSF shall provide a capability to verify the evidence of origin of information to *the receiving SSL peer* given [the successful establishment of a SSL session].

Cryptographic Support (FCS)

FCS_CKM.1(1) Cryptographic Key Generation - RSA

FCS_CKM.1.1(1)	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [512, 1024 bits] that meet the following: [PKCS #1 Version 1.5].

FCS_CKM.1(2) Cryptographic Key Generation – Diffie-Hellman

FCS_CKM.1.1(2)	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Diffie-Hellman Key agreement] and specified cryptographic key sizes [768, 1024, or 1536 bits] that meet the following: [PKCS #3].

FCS_CKM.4(1) Cryptographic Key Destruction

FCS_CKM.4.1(1)	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite with zeroes] that meets the following: [no standard].

FCS_COP.1(1) Cryptographic Operation - Encryption

FCS_COP.1.1(1)	The TSF shall perform [bulk encryption and decryption] in accordance with a specified cryptographic algorithm [Triple DES, AES] and cryptographic key sizes [168 bit for Triple DES, and 128, 192, and 256 bit for AES] that meet the following: [FIPS 46-3, FIPS 197]

FCS_COP.1(2) Cryptographic Operation—Hashed Message Authentication Code Generation

FCS_COP.1.1(2) The TSF shall perform [HMAC generation] in accordance with a specified cryptographic algorithm [SHA-1, MD5] and cryptographic key sizes [160 bit, 128 bit] that meet the following: [RFC 2404, RFC 2403, RFC 2246]

FCS_COP.1(3) Cryptographic Operation— Remote Administration

FCS_COP.1.1(3) The TSF shall perform [encryption of remote authorization administrator sessions] in accordance with a specified cryptographic algorithm [Triple DES as specified in FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are in dependent keys) or AES as specified in FIPS PUB 197] and cryptographic key sizes [that are 192 binary digits in length] that meet the following: [FIPS PUB 46-3 with Keying Option 1 (for DES) or FIPS PUB 197 (for AES) and FIPS PUB 140-1 (Level 1) or FIPS PUB 140-2 (Level 1)].

FCS_COP.1(4) Cryptographic Operation—SCEP Signing

FCS_COP.1.1(4) The TSF shall perform [digital signing and signature verification] in accordance with a specified cryptographic algorithm [MD5 with RSA Encryption] and cryptographic key sizes [128, 512, or 1024 bits] that meet the following: [PKCS#1, PKCS#10].

FCS_COP.1(5) Cryptographic Operation—SCEP Encryption

FCS_COP.1.1(5) The TSF shall perform [encryption/decryption] in accordance with a specified cryptographic algorithm [3DES CBC] and cryptographic key sizes [168 bits] that meet the following: [FIPS 46-3].

User Data Protection (FDP)

FDP_IFC.1(1) Subset Information Flow Control—IPSec

FDP_IFC.1.1(1) The TSF shall enforce the [IPSec information flow control SFP] on [subjects: IP network devices
Information: IP packet
Operations: encrypt, decrypt, or ignore, permit, deny].

FDP_IFC.1(2) Subset Information Flow Control—SSL

FDP_IFC.1.1(2) The TSF shall enforce the [SSL information flow control SFP] on [subjects: IP network devices
Information: IP Packet
Operations: permit or deny].

FDP_IFF.1(1) Simple Security Attributes—IPSec

FDP_IFF.1.1(1) The TSF shall enforce the [IPSec information flow control SFP] based on the following types of subject and information security attributes: [

SubjectSecurity Attributes

- Presumed address.

Information Security Attributes

- Source/destination IP address;
- Source/destination port number;
- IPSec Security association;
- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- network layer protocol;
- TOE interface on which traffic arrives and departs

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

1. If subject can authenticate with the TOE during the IKE negotiation and establish an IPSec Security Association based on VPN security attributes created by the authorized administrator].

FDP_IFF.1.3(1) The TSF shall enforce [the following rules once the IPSec tunnel is established:

a) Incoming IPSec-encapsulated traffic shall be decrypted per FCS_COP.1(1) based on tunnel crypto access control list established by the authorized administrator and security association.

b) Outgoing traffic shall be encrypted per FCS_COP.1(1) based on tunnel crypto access control list established by the authorized administrator and security association and tunneled to the VPN peer corresponding to the destination address.]

FDP_IFF.1.4(1) The TSF shall provide [inbound packet filtering based on interface access control lists to filter on presumed source/destination IP address, protocol, interface and source/destination port number as configured by the administrator such that:

Subjects on the external network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an external network address;
- and the presumed address of the destination subject, in the information, translates to an address on another connected network].

FDP_IFF.1.5(1) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6(1) The TSF shall explicitly deny an information flow based on the following rules: [

1. The TSF shall reject inbound packets in clear text if the source address is not explicitly allowed to send information in the clear text.

2. The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

3. The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject

is an external IT entity on the external network;

4. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

5. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.]

FDP_IFF.1(2) Simple Security Attributes—SSL

FDP_IFF.1.1(2) The TSF shall enforce the [SSL information flow control SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes

- Presumed address.

Information Security Attributes

- Source/destination IP address;,
- Source/destination port number;
- SSL security parameters,
- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- network layer protocol;
- TOE interface on which traffic arrives and departs].

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

1) If subject can successfully authenticate during SSL negotiation (handshake) and negotiate SSL security parameters with the TOE based on SSL security attributes created by the authorized administrator].

FDP_IFF.1.3(2) The TSF shall enforce [the following rules once the SSL tunnel is established: The TSF shall permit or deny the subject access to information based on SSL security attributes and access control lists defined by the tunnel group as configured by the authorized administrator].

FDP_IFF.1.4(2) The TSF shall provide [inbound packet filtering based on interface access control lists to filter on presumed source/destination IP address, protocol, interface and source/destination port number as configured by the administrator such that:

Subjects on the external network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an external network address;

- and the presumed address of the destination subject, in the information, translates to an address on another connected network].

FDP_IFF.1.5(2) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6(2) The TSF shall explicitly deny an information flow based on the following rules: [

1. The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

2. The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

3. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

4. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.].

FDP_UCT.1(1) Basic Data Exchange Confidentiality—IPSec

FDP_UCT.1.1(1) The TSF shall enforce the [IPSec information flow control SFP] to be able to *transmit and receive* objects in a manner protected from unauthorized disclosure.

FDP_UCT.1(2) Basic Data Exchange Confidentiality—SSL

FDP_UCT.1.1(2) The TSF shall enforce the [SSL information flow control SFP] to be able to *transmit and receive* objects in a manner protected from unauthorized disclosure.

FDP_UIT.1(1) Data Exchange Integrity—IPSec

FDP_UIT.1.1(1) The TSF shall enforce the [IPSec information flow control SFP] to be able to *transmit and receive* user data in a manner protected from *modification, insertion,* ***and*** *replay* errors.

FDP_UIT.1.2(1) The TSF shall be able to determine on receipt of user data whether *modification, insertion,* ***and*** *replay* **have** occurred.

FDP_UIT.1(2) Data Exchange Integrity—SSL

FDP_UIT.1.1(2) The TSF shall enforce the [SSL information flow control SFP] to be able to *transmit and receive* user data in a manner protected from *modification, insertion,* ***and*** *replay* errors.

FDP_UIT.1.2(2) The TSF shall be able to determine on receipt of user data whether *modification, insertion,* ***and*** *replay* **have** occurred.

Identification and Authentication (FIA)

FIA_UAU.2 User Authentication Before Any Action

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

FIA_UAU.5(1) Multiple Authentication Mechanisms[1]

FIA_UAU.5.1(1) The TSF shall provide [reusable password and certificate-based authentication mechanisms] to support user authentication.

FIA_UAU.5.2(1) The TSF shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules:

a) password authentication mechanism shall be used for authorized administrators to access the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator.

b) if configured, certificate-based authentication mechanism shall be used for VPN users accessing the TOE to establish an SSL VPN session such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that VPN user.

c) Reusable password mechanism shall be used for authorized human users to access the TOE to establish a VPN session such that successful authentication must be achieved before allowing any other TSF-mediated actions].

Application Note If the TOE is configured to use an external authentication server, the TOE shall be responsible for correctly invoking the external authentication mechanism, and for taking the correct actions based on authentication decisions. In keeping with industry practice the choice of authentication server is not mandated by this ST.

FIA_UID.2(1) User Identification Before Any Action

FIA_UID.2.1(1) The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Security Management (FMT)

FMT_MOF.1(1) Management of Security Functions Behavior

FMT_MOF.1.1(1) The TSF shall restrict the ability to *enable* ***and*** *disable* the functions [:

a) VPN operation of the TOE;

b) use of an external authentication server;

c) use of a certificate authority server] to [an authorized administrator].

1. Note items b) and c) of this security functional requirement may be partially addressed by the TOE environment if configured by the authorized administrator.

FMT_MOF.1(2) Management of Security Functions Behavior

FMT_MOF.1.1 (2) The TSF shall restrict the ability to *determine the behavior of, enable, disable, **and** modify the behavior of* the functions [:

a) that implement the IPSec information flow control SFP;

b) that implement the SSL information flow control SFP;

c) backup and restore of TSF data, information flow rules, and audit trail data; and

d) communication of authorized external IT entities with the TOE] to [an authorized administrator].

Application Note Determine and modify the behavior of element d) (communication of authorized external IT entities with the TOE) is intended to cover functionality such as providing a range of addresses from which the authorized external entity can connect.

FMT_MSA.1 (1) Management of Security Attributes—IPSec

FMT_MSA.1.1 (1) The TSF shall enforce the [IPSec information flow control SFP] to restrict the ability to *modify **attributes in a rule and** delete **attributes in a rule*** the security attributes [listed in FDP_IFF.1(1)] to [the authorized administrator].

FMT_MSA.1 (2) Management of Security Attributes—SSL

FMT_MSA.1.1 (2) The TSF shall enforce the [SSL information flow control SFP] to restrict the ability to *modify **attributes in a rule and** delete **attributes in a rule*** the security attributes [listed in section FDP_IFF.1(2)] to [the authorized administrator].

FMT_MSA.2(1) Secure Security Attributes

FMT_MSA.2.1(1) The TSF shall ensure that only secure values are acceptable for security attributes.

FMT_MSA.3 Static Attribute Initialization

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

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

FMT_MTD.1(1) Management of TSF Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to *delete, clear,* **and** *[load]* the [IPSec Pre-Shared Keys and certificates] to [the authorized administrator].

FMT_MTD.1(2) Management of TSF Data

FMT_MTD.1.1(2) The TSF shall restrict the ability to *modify, delete,* **and** *[add]* the [user-oriented SSL attributes, and user and password identity credentials] to [the authorized administrator].

FMT_MTD.1(3) Management of TSF Data

FMT_MTD.1.1(3) The TSF shall restrict the ability to *change_default, clear,* **and** *[specify]* the [IPSec configuration attributes and SSL configuration attributes] to [the authorized administrator].

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

[a) Enable or disable the VPN operation of the TOE

b) Enable or disable use of an external authentication server

c) Enable, disable, determine and modify the behavior of the functions that implement the IPSec information flow control SFP

d) Enable, disable, determine and modify the behavior of the functions that implement the SSL information flow control SFP

e) Enable, disable, determine and modify the behavior of the backup and restore function for TSF data, information flow rules, and audit trail data

f) Enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE

g) Modify and delete attributes in a rule for security attributes listed in section FDP_IFF1.1(1) and FDP_IFF1.1(2)

h) Delete, clear, and load IPSec Pre-Shared Keys

i) Modify, delete, and add user-oriented SSL attributes and user and password identity credentials

j) Change_default, clear, and specify IPSec configuration attributes and SSL configuration attributes

k) Read audit records

l) Enable or disable use of a certificate authority server].

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [authorized administrator, VPN user].

FMT_SMR.1.2 The TSF shall be able to associate **human** users with **the authorized administrator and VPN user** roles.

Protection of the TSF (FPT)

FPT_AMT.1 Abstract Machine Testing

FPT_AMT.1.1 The TSF shall run a suite of self tests *during initial start-up* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Dependencies: No dependencies

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1	The TSF shall protect TSF data from *disclosure* **and** *modification* when it is transmitted between separate parts of the TOE.

FPT_RVM.1(1) Non-Bypassability of the TSP

FPT_RVM.1.1(1)	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Application Note This requirement only applies to the ASA component of the TOE.

FPT_SEP.1(1) TSF Domain Separation

FPT_SEP.1.1(1)	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FMT_SEP.1.2(1)	The TSF shall enforce separation between the security domains of subjects in the TSC.

Application Note This requirement only applies to the ASA component of the TOE.

FPT_STM.1 Reliable Time Stamps

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

Application Note The word "reliable" in the above requirement means that the order of the occurrence of auditable events is preserved. Reliable time stamps, which include both date and time, are especially important for TOEs comprised of greater than one component.

FPT_TST.1 TSF Testing

FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up* to demonstrate the correct operation of *the TSF*.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of *TSF data*.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Application Note This requirement only applies to the ASA component of the TOE.

TOE Access (FTA)

FTA_TSE.1 TOE Session Establishment

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

Trusted Path/Channel (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of it end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [the TSF and trusted IT product] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [the secure transmission of IPSec packet flows for LAN-to-LAN VPN, external authentication services, and external certificate authority services].

Application Note The TOE can be configured to use local authentication mechanisms or use authentication services provided by an external authentication server. The use of an external authentication server is optional in all TOE configurations, and not required for any TOE configuration. The TOE shall be responsible for correctly invoking the external authentication mechanism, and for taking the correct actions based on authentication decisions. In keeping with industry practice the choice of authentication server is not mandated by this ST.
The TOE can be optionally configured to use an external certificate authority service.

FTP_RTC.1 Remote Administration Trusted Channel (EXP)

FTP_RTC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure
FTP_RTC.1.2	The TSF shall permit the remote IT trusted product to initiate communication via the trusted channel.
FTP_RTC.1.3	The TSF shall use a trusted channel for the following functions: secure remote administration

Security Requirements for the IT Environment

The following functional requirements are met partially by the TOE and partially by the IT Environment.

Table 8 Security Functional Requirements for the TOE IT Environment

Functional Component	
FCS_CKM.1(3)	Cryptographic Key Generation - RSA
FCS_CKM.1(4)	Cryptographic Key Generation – Diffie-Hellman
FCS_CKM.4(2)	Cryptographic Key Destruction
FCS_COP.1(6)	Cryptographic Operation – Encryption
FCS_COP.1(7)	Cryptographic Operation – Hashed Message Authentication Code Generation
FIA_UAU.5(2)	Multiple Authentication Mechanisms

Table 8 Security Functional Requirements for the TOE IT Environment

Functional Component	
FIA_UID.2(2)	User Identification Before Any Action
FMT_MSA.2(2)	Secure Security Attributes
FPT_RVM.1(2)	Non-Bypassability of the TSP
FPT_SEP.1(2)	TSF Domain Separation

Cryptographic Support (FCS)

FCS_CKM.1(3) Cryptographic Key Generation—RSA

FCS_CKM.1.1(3) The **IT Environment of the SSL Host OS Component** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [512, 1024 bits] that meet the following: [PKCS #1, Version 1.5].

FCS_CKM.1(4) Cryptographic Key Generation—Diffie-Hellman

FCS_CKM.1.1(4) The **IT Environment of the SSL Host OS Component** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Diffie-Hellman Key agreement] and specified cryptographic key sizes [768, 1024, or 1536 bits] that meet the following: [PKCS #3].

FCS_CKM.4(2) Cryptographic Key Destruction

FCS_CKM.4.1(2) The **IT Environment of the SSL Host OS Component** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite with zeroes] that meets the following: [no standard].

FCS_COP.1(6) Cryptographic Operation—Encryption

FCS_COP.1.1(6) The **IT Environment of the SSL Host OS Component** shall perform [bulk encryption and decryption for SSL 3.0 or TLS 1.0] in accordance with a specified cryptographic algorithm [Triple DES, AES] and cryptographic key sizes [168 bit, 256 bit] that meet the following: [FIPS 46-3, FIPS 197]

FCS_COP.1(7) Cryptographic Operation—Hashed Message Authentication Code Generation

FCS_COP.1.1(7) The **IT Environment of the SSL Host OS Component** shall perform [HMAC Generation] in accordance with a specified cryptographic algorithm [SHA-1, MD5] and cryptographic key sizes [160 bit, 128 bit] that meet the following: [RFC 2246]

Identification and Authentication (FIA)

FIA_UAU.5(2) Multiple Authentication Mechanisms[2]

FIA_UAU.5.1(2) The **IT environment** shall provide [reusable password and certificate-based authentication mechanisms] to support user authentication.

2. Note that items a, b) and c) of this security functional requirement are addressed partially by the TOE environment.

FIA_UAU.5.2(2) The **IT environment** shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules:

a) password authentication mechanism shall be used for authorized administrators to access the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator.

b) if configured, certificate-based authentication mechanism shall be used for VPN users accessing the TOE to establish an SSL VPN session such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that VPN users.

c) Reusable password mechanism shall be used for authorized human users to access the TOE to establish a VPN session such that successful authentication must be achieved before allowing any other TSF-mediated actions].

Application Note If the TOE is configured to use an external authentication server, the TOE shall be responsible for correctly invoking the external authentication mechanism, and for taking the correct actions based on authentication decisions. In keeping with industry practice the choice of authentication server is not mandated by this ST.

FIA_UID.2(2) User identification before any action

FIA_UID.2.1(2) The **IT environment** shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

Security Management (FMT)

FMT_MSA.2(2) Secure Security Attributes

FMT_MSA.2.1(2) The **IT Environment of the SSL Host OS Component** shall ensure that only secure values are acceptable for security attributes.

Protection of the TSF (FPT)

FPT_RVM.1(2) Non-Bypassability of the TSP

FPT_RVM.1.1(2) The **IT environment** shall ensure that **VPN Client Components** enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1(2) TSF Domain Separation

FPT_SEP.1.1(2) The **IT environment** shall maintain a security domain for its own execution that protects it **and the VPN Client Components** from interference and tampering by untrusted subjects.

FPT_SEP.1.2(2) The **IT environment** shall enforce separation between the security domains of subjects in the TSC.

TOE Security Assurance Requirements

The TOE security assurance requirements summarized in Table 9 identify the management and evaluative activities required to address the threats and policies identified in the "Security Environment" section on page 14 of this ST. These assurance requirements compose an Evaluation Assurance Level 4 (EAL4) augmented with ALC_FLR.1 (Basic Flaw Remediation).

Table 9 TOE Assurance Requirements

Assurance Class	Component ID	Component Description
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User Guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Basic Flaw Remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Developer vulnerability analysis

SFRs With SOF Declarations

The claimed minimum strength of function for the TOE is SOF-basic.

The only probabilistic or permutational mechanism in the TOE is the password mechanisms used to authenticate the users. The SFRs that specifies this mechanism is FIA_UAU.2 and FIA_UAU.5.

TOE Summary Specification

This section identifies and describes the security functions implemented by the TOE and the assurance measures applied to ensure their correct implementation.

TOE Security Functions

Security Management Function

Functional Requirements satisfied: FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.2(1), FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMF.1, FMT_SMR.1, FTP_RTC.1.

The Security Management Function provides a command line interface (CLI) that allows an authorized administrator to configure security functionality on the TOE either locally via the console port or remotely using SSH to perform the following actions:

1. Enable or disable the VPN operation of the TOE;
2. Enable or disable use of an external authentication server;
3. Enable, disable, determine and modify the behavior of the functions that implement the IPSec information flow control SFP;
4. Enable, disable, determine and modify the behavior of the functions that implement the SSL information flow control SFP;
5. Enable, disable, determine and modify the behavior of the audit trail data;
6. Enable, disable, determine and modify the behavior of the backup and restore function for TSF data, and information flow rules;
7. Enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE;
8. Modify and delete attributes in information flow rules for IPSec and SSL VPN;
9. Modify, delete, and clear IPSec Pre-Shared Keys;
10. modify, delete, and add user-oriented SSL attributes and user and password identity credentials;
11. change_default, clear, and specify IPSec configuration attributes and SSL configuration attributes;
12. read audit records; and
13. Enable and disable use of a certificate authority server.

Upon successful identification and authentication, the administrator has access to the CLI that enables an administrator to manage and monitor the TOE. The CLI is divided into different command modes. Each command mode has its own set of commands available for the configuration, maintenance, and monitoring of the TOE. The commands available depend on the current active mode. The use of specific commands allows navigation from one command mode to another. The command modes are grouped into two categories based on the Authorized Administrator role; “unprivileged” is where an administrator can view configuration information but cannot change it, and “privileged” which provides the ability to change configuration information. Upon successful login, by default, the administrator can access the unprivileged CLI commands. When the administrator authenticates with the enable or login command, the administrator has access to privileged modes and commands. Though the administrator

could also use the unprivileged mode, all TOE relevant administrative operations are performed in a privileged mode. The above listed management functions can only be performed by the authorized administrator in a privileged mode.

The Security Management Function ensures that validated security attributes are entered by an authenticated administrator.

The Security Management Security Function also maintains the VPN user role as stated in FMT_SMR.1 by maintaining a list of allowed remote VPN users that can establish a VPN connection The VPN user represents the user which utilizes the TOE to establish VPN access to network resources on the protected network. The VPN user's interface is limited to identification and authentication interactions to determine whether the user is allowed to establish the VPN connection. .

> **Groups and VPN users are core concepts in configuring and managing the security of VPNs. They specify attributes that determine VPN user access to and use of the VPN (both IPSec and SSL VPNs). A group is a collection of VPN users treated as a single entity. VPN users get their attributes from group policies. Tunnel groups identify the group policy for a specific VPN connection and consists of a set of records that determines tunnel connection policies. Group policies define user-oriented attributes that set terms for user connections after the VPN connection is established. If a particular group policy is not assigned to a VPN user, a default group policy for the connection applies. Tunnel groups and group policies simplify security management. To streamline configuration, the TOE provides a default LAN-to-LAN tunnel group, a default remote access (IPSec) tunnel group, a default WebVPN tunnel group, and a default group policy. The default tunnel group and group policy provide settings that are likely to be common for many VPN users. By default, VPN users inherit all user attributes fm the assigned group policy. The TOE also lets the authorized administrator assign individual attributes (user-specific) to the user thus overriding values in the group policy that applies to that user. The user-oriented SSL attributes, IPSec configuration attributes and SSL configuration attributes are captured in the tunnel group policies, group policies, and user-specific policy. Audit Function**

Functional Requirements: FAU_GEN.1, FAU_SAR.1, FPT_STM.1

The TOE generates audit records (system messages) for the following types of events: errors during IPSec processing, errors during SSL processing, decisions on request for information flow, and failures during digital certificate processing. These events are generated by the TOE immediately upon occurrence by calling the logging facility within the TOE.

For each event the Audit Function will record the following:

1. Date and time of the event;
2. Source and destination IP address (for connections only);
3. Type of event or service;
4. Specific information related to the event;
5. Success or failure of the event.

Audit records can be viewed by the authorized administrator via the CLI using show logging command. Audit records are stored on the ASA in an internal syslog buffer.

IPSec VPN Function

Functional Requirements: FCO_NRO.2, FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.4(1), FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(4), FCS_COP.1(5), FDP_IFC.1, FDP_IFF.1, FDP_UCT.1, FDP_UIT.1, FTA_TSE.1, FTP_ITC.1, FIA_UAU.5(1), FPT_ITT.1.

The IPSec VPN Function includes both IPSec and Internet Security Association and Key Management Protocol (ISAKMP) functionality to support VPNs. A secure connection between two IPSec peers is called a tunnel. The TOE implements ISAKMP and IPSec tunneling standards to build and manage VPN tunnels. ISAKMP and IPSec accomplish the following:

- Negotiate tunnel parameters
- Establish tunnels
- Authenticate users
- Encrypt and decrypt data
- Manage data transfer across the tunnel.

IPSec provides authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE implementation of the IPSec standard (RFCs 2401-2410) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption, and anti-replay services. The TOE implements IPSec in two types of configurations:

- LAN-to-LAN configurations are between two IPSec security gateways, such as security appliance units or other protocol-compliant VPN devices. A LAN-to-LAN VPN connects networks in different geographic locations.
- Remote access configurations provide secure remote access for Cisco VPN clients, such as mobile users. A remote access VPN lets remote users securely access centralized network resources. The Cisco VPN client complies with the IPSec protocol and is specifically designed to work with the TOE.

In IPSec LAN-to-LAN connections, the TOE can function as initiator or responder. In IPSec remote access connections, the ASA functions only as responder. Initiators propose Security Associations (SAs); responders accept, reject, or make counter-proposals—all in accordance with configured SA parameters. To establish a connection, both entities must agree on the SAs.

The TOE IPSec implementation contains a number of functional components that comprise the IPSec VPN function. In IPSec terminology, a peer is a remote-access client or another secure gateway.

Additionally the TOE performs input packet filtering by applying an access-control list (ACLs) to specific interfaces of the ASA. Interface ACLs filter network traffic by controlling whether routed packets are forwarded (permit) or dropped (deny). The TOE examines each packet to determine whether to forward or drop the packet, on the basis of the criteria the authorized administrator specified within the ACLs. The access-control list can include transport protocol, IP protocol, network protocol, source/destination IP address and source/destination UDP/TCP port number. Packets not matching the access-list are logged and discarded by the ASA. By default, the TOE denies all packets on the originating interface unless permit access is specifically set in the ACL. An ACL can contain one or more Access Control Entry (ACEs). The order of ACEs is important. When the TOE decides whether to forward or drop a packet, the TOE tests the packet against the ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked such that if the ACE at the beginning of the ACL explicitly permits all traffic, no further ACEs are checked. Interface ACLs are applied first before IPsec negotiations occur in the evaluated configuration. The functionality provided by Interface ACLs is modeled in the IPSec Information Flow SFP.

IPSEC.1—IPSec Internet Key Exchange (IKE)

IPSec Internet Key Exchange, also called ISAKMP, is the negotiation protocol that lets two peers agree on how to build an IPSec SA. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPSec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPSec peers that is also used to manage IPSec connections, including:

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

An ISAKMP policy includes an authentication method, encryption method, HMAC method, a Diffie-Hellman group and a policy lifetime. When IKE negotiations begin, the peer that initiates the negotiation sends all of its policies to the remote peer. The remote peer checks all the peer's policies against each of its configured polices in priority order (highest priority first) until it discovers a match. A match exists when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer policy specifies a lifetime less than or equal to the lifetime in the policy of the initiator. IKE authenticates IPSec peers using pre-shared keys, RSA keys or digital certificates. It also handles the generation and agreement of secure session keys using the Diffie-Hellman algorithm and negotiates the parameters used during IPSec ESP (IPSEC.2). The TOE generates secure RSA public/private keys (512 and 1024 bit key lengths) for use with a Public Key Infrastructure (PKI). If configured by the authorized administrator, 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. This can be done during TOE installation or while the TOE is operational. The TOE can destroy keys it creates by overwriting them.

After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation.

IPSec tunnels are sets of IPSec SAs that the TOE establishes between peers. The SAs define the security settings to apply to sensitive data, and also specify the keying material the peers use. The peers negotiate the settings to use for each SA during Phase 2. Each SA consists of transform sets and crypto maps. A transform set is a combination of security settings that define how the TOE protects data. During IPSec SA negotiations (Phase 2), the peers must identify a transform set that is the same as at both peers. The TOE then applies the matching transform set to create an SA that protects data flows as specified by the crypto map ACL for the associated crypto map (IPSEC.2). For two peers to succeed in establishing an SA, they must have at least one compatible (match) crypto map (IPSEC.3).

IKE extended authentication (Xauth) is a draft RFC based on the IKE protocol and requires username and password to perform user authentication in a separate phase after the IKE authentication phase 1 exchange. Xauth does not replace IKE. IKE allows for device authentication (using pre-shared keys, RSA keys or digital certificates) and Xauth allows for VPN user authentication, which occurs after IKE device (peer) authentication. Xauth occurs after IKE phase 1 but before IKE IPSec SA negotiation phase 2. The TOE can be configured to use the local authentication mechanism or an external authentication server for Xauth user authentication.

IPSEC.2—IPSec Encapsulating Security Payload (ESP)

The TOE uses ESP to protect packet flows between IPSec peers across interconnected untrusted networks in accordance with a TOE security policy (TSP). ESP is a method of encapsulating IP Packets and provides confidentiality using the 3DES and AES ciphers, integrity and authenticity using the MD5 and SHA-1 algorithms, and a mechanism to detect the capture and retransmission of packets (replay attacks) ensuring proof of origin cannot be repudiated.

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

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

IPSEC.3—Cryptographic Maps

Cryptographic Maps (crypto maps) are used by the TOE to specify:

a) the packet flow (i.e.. IP packets) that are to be protected by encryption, identified by cryptoanACL that can include IP protocol, source/destination IP address and source/destination UDP/TCP port number;

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

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

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

With IPSec, the administrator defines what traffic should be protected between two IPSec peers by configuring crypto map ACLs and applying these access lists to interfaces by way of cryptographic (crypto) map sets. Crypto map ACLs are used to specify what traffic to protect based on source and destination address. (The crypto map ACLs used for IPSec are used only to determine which traffic should be protected by IPSec, not which traffic should be dropped or forwarded through the interface. Separate interface ACLs define dropping and forwarding at the interface.) Crypto maps define the IPSec policy to be negotiated in the IPSec SA. They include an ACL, peer identification, local address for IPSec traffic, and up to six transform sets with which to attempt to match the peer security settings. A crypto map set can contain multiple entries (crypto map), each with a different crypto map access control list. The crypto map entries are searched in order and the TOE attempts to match the packet to the crypto map access control list specified in that entry. The administrator must assign a Crypto map set to each interface through which IPSec traffic flow. Assigning the crypto map set to an interface instructs the TOE to evaluate all traffic against the crypto map set and to use the specified policy during connection or SA negotiation.

The IPSec policy to allow the IPSec VPN tunnel requires the user to be successfully authenticated. The ASA uses username/password to authenticate the user. If configured by the authorized administrator, the ASA can use an external authentication server to perform the authentication. The VPN client and ASA negotiate how to build the IPSec security association by first authenticating each other using the pre-shared keys or certificates (RSA). Once the security associations are negotiated and the IPSec tunnel is successfully established, the ASA encrypts packets based on the crypto map ACLs in the security associations. The ASA permits (protects) and denies (passes without encrypting) specific traffic through the tunnel based on cryptomap ACLs configured by the authorized administrator. Like interface ACLs, the crypto mapACLs contain ACEs. ACEs containing deny statements filter out outbound traffic that does not require IPSec protection and passes the packet with encrypting it. For an inbound, encrypted packet, the TOE decrypts the packet, and compares the inner header of the decrypted packet to the permit ACEs in the crypto map ACL associated with the packet SA. If the inner header fails to match the ACE, the TOE drops the packet. If it matches, the TOE forwards the packet.

SSL VPN Function

Functional Requirements: FCO_NRO.2(2), FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.4(1), FCS_COP.1(1), FCS_COP.1(2), FDP_IFC.1(2), FDP_IFF.(2), FDP_UCT.1(2), FDP_UIT.1(2), FPT_ITT.1, FIA_UAU.5(1)

The SSL VPN lets users establish a secure, remote-access VPN tunnel to the TOE by using the SSL and TLS protocol. The end user must first access the ASA component by using an SSL-capable web browser. Establishing an SSL VPN session requires the following:

- Use of HTTPS to access the TOE. In a Web browser, remote users enter the TOE IP address in the format *https://address* where address is the IP address or DNS hostname of the TOE interface. This is referred to as WebVPN Authentication
- Administrator enabling WebVPN sessions on the TOE interface that remote users connect to.

SSL uses digital certificates for device authentication. The TOE creates a self-signed SSL server certificate when it boots, or the administrator can install in the TOE an SSL certificate that has been issued by a defined trust point (i.e., Certificate Authority). For HTTPS, this certificate must be then be installed on the remote host

The user is prompted to enter a username and password. If configured, the user can be authenticated using a digital certificate. A RADIUS server or internal authentication server can be used to authenticate remote users. Once the user successfully authenticates to the TOE, the user continues the connection using a clientless VPN connection (WebVPN). WebVPN provides easy access to a broad range of web resources and web-enabled applications from almost any computer on the Internet. These include secure access to the following resources:

- Internal web sites
- Web-enabled applications
- NT/Active Directory file shares
- Email proxies, including POP3S, IMAP4S, and SMTPS

WebVPN uses the SSL protocol and its successor, Transport Layer Security (TLS) to provide a secure connection between remote users and specific, supported internal resources as configured by the administrator. The TOE recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users. Remote users have no direct access to resources on the internal network. The administrator can control what applications and URLs the user can access by identifying allowed applications and urls within user-oriented SSL security attributes. Permitted WebVPN traffic flows are also determined by ACLs defined within a group policy for a WebVPN tunnel group.

SSL is designed not as a single protocol but rather two layers of protocols:

- SSL Record Protocol which provides the basic security services to various higher-level protocols. The SSL Protocol provides two services for SSL connections-encrypting application data using triple DES or AES and message integrity using a message authentication code (HMAC).
- SSL-Specific Protocols is used in the management of SSL exchanges. The Handshake protocol is the most complex part of SSL and allows the TOE and the client to authenticate each other to negotiate the following SSL security parameters: an encryption (triple DES or AES) and MAC algorithm, key exchange method (RSA, Diffie-Hellman), and cryptographic keys to be used to protect data sent in an SSL record. The Handshake protocol is used before any application data is transmitted.

Additionally the TOE performs inbound packet filtering by applying an access-control list to specific interfaces of the ASA. Interface ACLs filter network traffic by controlling whether routed packets are forwarded (permit) or dropped (deny). The TOE examines each packet to determine whether to forward or drop the packet, on the basis of the criteria the authorized administrator specified within the ACLs. The access-control list can include transport protocol, IP protocol, network protocol, source/destination IP address and source/destination UDP/TCP port number. Packets not matching the access-list are logged and discarded by the ASA unless a specific rule has been set up to let the packet pass. Interface ACLs are applied first before WebVPN group policy defined ACLs. The functionality provided by access-control lists is modeled in the SSL Information Flow SFP.

Identification and Authentication Function

Functional Requirements: FIA_UAU.2, FIA_UAU.5(1), FIA_UID.2(1), FCS_CKM.1(1), FCS_COP.1(3), FTP_RTC.1, FTP_ITC.1

The TOE maintains the authorized administrator and VPN Client user roles. The VPN user is required to be successfully identified and authenticated with a user name and password or, if configured, by certificate for SSL VPN before a VPN connection can be established. The TOE is configured to authenticate the administrator for both unprivileged and privileged access to the CLI using a username and password. The TOE shall be configured to require an access password, which provides unprivileged access and an enable password which provides privileged access. Privileged access is defined by any privilege level entering an enable password after their individual login. The TOE restricts the ability to create, modify and delete user accounts to administrators. No CLI functions are accessible to an unauthenticated user, with the exception of the authentication functions. Additionally unprivileged access restricts the administrator from accessing any CLI commands that modify the security configuration of the TOE. Administrators are required to identify themselves and be authenticated before any further access to the TOE is granted (i.e. before they become authorized administrators). The Identification and Authentication Function provides the TOE interfaces to allow an authorized administrator to log into the TOE locally or remotely. Remote access is protected via SSH.

Authentication performed by the TOE makes use of a reusable password mechanism for access to the TOE by authorized administrators as well as by human users establishing VPN connections. This is a permutational mechanism that meets the minimum strength of function rating of SOF-basic. The TOE by default is configured to perform local authentication and stores user names and passwords in an internal user authentication database which is only accessible by the administrator via privileged commands. The TOE can be configured to use an external authentication server such that the TOE is responsible for correctly invoking the external authentication mechanism, and for taking the correct actions based on the external server's authentication decisions.

If configured, certificate-based authentication for a VPN user to establish an SSL VPN tunnel is supported by the TOE. The authorized administrator could configure the TOE to handle the authentication locally or by using an external authentication server in the TOE environment.

Self-Protection Function

Functional Requirements: FPT_AMT.1, FPT_RVM.1(1), FPT_SEP.1(1), FPT_TST.1, FPT_ITT.1, FDP_IFF.(1), FDP_IFF.(2)

The Self-Protection Function provides a multitasking environment for the ASA. Within this environment all processes are allocated separate memory locations within the RAM. Whenever memory is re-allocated it is flushed of data prior to re-allocation. The ASA accounts for all packets traversing the TOE in relation to the associated information stream. Therefore no residual information relating to other packets will be reused on that stream.

The Self-Protection Function enforces the protection of the TOE configuration through the distinction and separation of information flows. All traffic arriving at a TOE interface is mediated by the TSF by the IPSec and SSL information flow policies and inbound packet filtering rules. The TOE protects itself from interference and tampering by untrusted subjects by implementing authentication and access controls to limit configuration to authorized administrators.

The remote management connection to the CLI via SSH must be explicitly enabled to be used and all other remote management connections that the TOE is capable of using, such as telnet, are disallowed in the evaluated configuration. The management interface presented at the console port is always enabled. Access to the CLI requires valid authentication. SNMP, telnet, and XML management interfaces are not enabled in the evaluated configuration described in this ST.

Self-Protection function also ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. This includes use of an encrypted link (with FIPS 140 validated cryptographic modules) for remote management functions

The ASA portion of the TOE performs self tests during initial start-up to verify that it is operating correctly. The TOE tests that the image installed has the expected MD5 hash to ensure the integrity of executable code. Further, the ASA performs cryptographic module testing. The Formula 1 operating system (F1OS) is not a general purpose operating system and access to F1OS memory space is restricted to only F1OS functions. Additionally, F1OS is the only software running on the TOE.

Clock Function

Functional Requirements: FPT_STM.1

The Clock Function of the TOE provides a source of date and time information for the TOE, used in audit timestamps and in validating service requests. This function can only be accessed from within the configuration exec mode via the privileged mode of operation of the ASA. The clock function is reliant on the system clock provided by the underlying hardware.

Assurance Measures

Table 10 identifies the deliverables that will meet the assurance requirements of Common Criteria EAL4, augmented with ALC_FLR.1. The identified deliverables describe the approach taken to meet the assurance requirements, and meet all of the assurance requirements contained in this assurance package.

Table 10 Assurance Measures

Assurance Class	Assurance Components	Assurance Measures (Cisco Documentation)
Configuration Management (ACM)	Partial CM Automation (ACM_AUT.1)	Configuration Management and Delivery Procedures for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). Installation Guide for the Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). Configuration Guide for the Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). The Configuration Management and Delivery Procedures describe the use of an automated configuration management system that meets the requirements of ACM_CAP.4 and ACM_AUT.1. All documentation required by ACM_SCP.1 is held under configuration control. These procedures also describe secure delivery process to preserve the integrity of the TOE, meeting the requirements of ADO_DEL.2 . The Installation Guide, Configuration Guide and Release Notes provide information on how to bring the delivered TOE into an operational state in accordance with ADO_IGS.1.
	Generation support and acceptance procedures (ACM_CAP.4)	
	Problem tracking CM coverage (ACM_SCP.2)	
Delivery and operation (ADO)	Detection of modification (ADO_DEL.2)	
	Installation, generation, and start-up procedures (ADO_IGS.1)	

Table 10 Assurance Measures (continued)

Assurance Class	Assurance Components	Assurance Measures (Cisco Documentation)
Development (ADV)	Fully defined external interfaces (ADV_FSP.2)	Functional Specification for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). This document describes the external interfaces to the TOE in a manner consistent with the requirements of ADV_FSP.2.
	Security enforcing high-level design (ADV_HLD.2)	High-level design for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). This document describes the TOE in terms of subsystems, and documents the interfaces between them.
	Subset of the implementation of the TSF (ADV_IMP.1)	Various source code for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). A sample of the TOE source code selected by the evaluators meets this requirement.
	Descriptive low-level design (ADV_LLD.1)	Low-level design for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). This document describes the decomposition of the TOE subsystems into modules, and documents the interfaces between them.
	Informal correspondence demonstration (ADV_RCR.1)	Correspondence demonstration for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). A description of correspondence between the TOE summary specification, the high-level design, the low-level design and source code is provided by means of cross-references in this document.
	Informal TOE security policy model (ADV_SPM.1)	Security Policy Model for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). The security policy model describes in an informal style the policies that underlie the TOE security functional requirements. These are traced to the functional specification.

Table 10 Assurance Measures (continued)

Assurance Class	Assurance Components	Assurance Measures (Cisco Documentation)
Guidance documents (AGD)	Administrator guidance (AGD_ADM.1)	Installation Guide for the Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). Configuration Guide for the Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). Command reference Guide for the Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). These documents provide detailed guidance on the administration of the TOE in a secure manner and user guidance for the VPN Client components. They also provide information on achieving the evaluated configuration.
	User guidance (AGD_USR.1)	
Life cycle support (ALC)	Identification of security measures (ALC_DVS.1)	Development Security for Cisco ASA Appliance, Cisco Adaptive Security Appliances Firewall Services Module (FWSM). This document defines the procedures used to maintain the security of the development environment. These measures provide a combination of procedural, personnel and technical measures that safeguard the integrity and confidentiality of the TOE.
	Basic flaw remediation (ALC_FLR.1)	Configuration and delivery procedures for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). This document describes the procedures and tools that are used in development and maintenance of the TOE. These procedures provide a controlled approach to management of the TOE life cycle. Procedures covering handling of reported flaws in the TOE are also provided.
	Developer defined life cycle model (ALC_LCD.1)	
	Well-defined development tools (ALC_TAT.1)	
Tests (ATE)	Analysis of coverage (ATE_COV.2)	Testing plan and analysis for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). The test documentation describes how each external security functional interface is tested, and also how it is demonstrated that the subsystem interfaces are also operating correctly. The documentation describes the test environments used, the tests that are carried out, and the results that are expected and obtained. The TOE is made available to the evaluators for testing.
	Testing: high-level design (ATE_DPT.1)	
	Functional testing (ATE_FUN.1)	
	Independent testing – sample (ATE_IND.2)	

Table 10 Assurance Measures (continued)

Assurance Class	Assurance Components	Assurance Measures (Cisco Documentation)
Vulnerability assessment (AVA)	Validation of analysis (AVA_MSU.2)	Misuse analysis for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). The misuse analysis provides an analysis of the guidance documentation, demonstrating that the TOE can be managed in a predictable and secure manner.
	Strength of TOE security function evaluation (AVA_SOF.1)	Strength of function analysis for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). The strength of function analysis provides an analysis of the password mechanism that demonstrates that the SOF claims are upheld.
	Independent Vulnerability Analysis (AVA_VLA.2)	Vulnerability analysis for Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540 and ASA-5550 Version 7.2(4). Cisco carries out and documents an analysis of the TOE deliverables searching for weaknesses that might allow an attacker to violate the TOE security policy. This analysis is provided to the evaluators.

Protection Profile Claims

This Security Target does not claim conformance to any registered protection profile.

Rationale

Security Objectives Rationale

This section demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective. Table 11 and Table 12 provide the mapping and rationale for the security objectives identified in the "Security Objectives" section on page 15 and the assumptions, threats and policies identified in the "Security Environment" section on page 14.

Table 11 Threats, Assumptions, and Policies to Security Objectives Mapping

	O.Authenticity	O.Confidentiality	O.Integrity	O.ID-Authentication	O.Key-Confidentiality	O.No-Replay	O.Secure-Operation	O.EAL	O.Audit-Record	O.Self-Protect	OE.Policy	OE.Secure-Management	OE.ID-Authentication	OE.Client
T.Audacc									X					
T.Attack							X					X		
T.Lowexp								X						
T.Untrusted Path	X	X	X		X	X								
T.No-Authentication				X									X	
T.Self-Protect										X				
A.No-Evil												X		
A.PhySec												X		
A.Training												X		
A.Trusted-CA												X		
A.PSK												X		
A.Host														X

Table 12 Threats, Assumptions, and Policies to Security Objectives Rationale

Threat/Assumption/ Policy	Security Objectives Rationale
T.Attack	The objectives (O.Secure-Operation, OE.Secure-Management) will provide an effective countermeasure as: • The TOE will be correctly configured in accordance with a security policy which will prevent bypass of the TSF; and • The TSP can only be altered by an authorized administrator from a secure management console.
T.Untrusted-Path	The objectives (O.Authenticity, O.Confidentiality, O.Integrity, O.Key-Confidentiality, O.No-Replay) will provide an effective countermeasure as: • O.Authenticity ensures that packet flows are received/transmitted from/to known, authenticated external IT entities and TOE; • O.Confidentiality ensures that the confidentiality of packet flows is maintained during transmission; • O.Integrity ensures that a packet flow cannot be modified without being detected by the TOE; • O.Key-Confidentiality ensures that cryptographic keys cannot be captured and used to decrypt packet flows; • O.No-Replay ensures that a packet flow transmitted to the TOE has not been copied by an eavesdropper and retransmitted to the TOE.
T.Audacc	The objective (O.Audit-Record) is necessary to counter this threat by requiring the generation of audit records into a readable audit trail.
T.Lowexp	The objective (O.EAL) is necessary to counter this threat because it requires that the TOE is resistant to penetration attacks performed by an attacker possessing low attack potential.
T.No-Authentication	The objective (O.ID-Authentication and OE.ID-Authentication) is necessary to counter this threat because it requires users to be uniquely identified and authenticated before accessing the TOE.
T.Self-Protect	The objective (O.Self-Protect) is necessary to counter the threat because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with the TSF.
A.No-Evil	The objective (OE.Secure-Management) upholds the assumption as: Those responsible for the operation of the TOE must ensure that management and configuration of the security functions of the TOE are undertaken by trusted staff that are non-hostile and follow all administrator guidance.
A.PhySec	The objective (OE.Secure-Management) upholds the assumption as: The TOE will be maintained in a location, which is physically secure.
A.Training	The objective (OE.Secure-Management) upholds the assumption as: Management and configuration of the security functions of the TOE are undertaken by trusted staff trained in the secure operation of the TOE

Table 12 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/Assumption/ Policy	Security Objectives Rationale
A.Trusted-CA	The objective (OE.Secure-Management) upholds the assumption as: Management and configuration of the security functions of the TOE are implemented in conjunction with trusted Certificate Authority (CA (i.e., a trusted third party or one that the organization trusts to manage certificate requests and issues digital certificates), if digital certificates are used for TOE authentication.
A.PSK	The objective (OE.Secure-Management) upholds the assumption as: Pre-shared Keys used for configuration in cryptographic maps are securely distributed amongst disparate administrators.
A.Host	The objective (OE.Client) upholds the assumption as: The VPN clients will be installed on a physically secure, properly configured and maintained IT platform.

Security Requirements Rationale

The purpose of this section is to show that the identified security requirements (Security Requirements, page 17) are *suitable* to meet the security objectives (Security Objectives, page 15). The following tables show that each security requirement (and SFRs in particular) is *necessary,* that is, each security objective is addressed by at least one security requirement, and vice versa.

Table 13 identifies each Security Requirement identified in the "TOE Security Functional Requirements" section on page 18 and the "TOE Security Assurance Requirements" section on page 32, and the TOE security objective(s) identified in the "Security Objectives for the TOE" section on page 16 that address it. Table 14 provides the mapping and rationale for inclusion of each requirement in this ST.

Table 13 TOE Security Requirement to TOE Security Objectives Mapping

	O.Authenticity	O.Confidentiality	O.Integrity	O.ID-Authentication	O.Key-Confidentiality	O.No-Replay	O.Secure-Operation	O.EAL	O.Audit-Record	O.Self-Protect
FAU_GEN.1							X		X	
FAU_SAR.1									X	
FCO_NRO.2(1)	X					X				
FCO_NRO.2(2)	X					X				
FCS_CKM.1(1)					X					
FCS_CKM.1(2)					X					
FCS_CKM.4(1)					X					
FCS_COP.1(1)		X								
FCS_COP.1(2)	X		X							

Table 13 TOE Security Requirement to TOE Security Objectives Mapping (continued)

	O.Authenticity	O.Confidentiality	O.Integrity	O.ID-Authentication	O.Key-Confidentiality	O.No-Replay	O.Secure-Operation	O.EAL	O.Audit-Record	O.Self-Protect
FCS_COP.1(3)							X			
FCS_COP.1(4)	X									
FCS_COP.1(5)	X									
FDP_IFC.1(1)	X	X	X		X	X				
FDP_IFC.1(2)	X	X	X		X	X				
FDP_IFF.1(1)	X	X	X		X	X				
FDP_IFF.1(2)	X	X	X		X	X				
FDP_UCT.1(1)		X								
FDP_UCT.1(2)		X								
FDP_UIT.1(1)			X							
FDP_UIT.1(2)			X							
FIA_UAU.2				X			X			
FIA_UAU.5(1)				X			X			
FIA_UID.2(1)				X			X			
FMT_MOF.1(1)							X			
FMT_MOF.1(2)							X			
FMT_MSA.1 (1)							X			
FMT_MSA.1 (2)							X			
FMT_MSA.2(1)		X	X		X		X			
FMT_MSA.3							X			
FMT_MTD.1(1)							X			
FMT_MTD.1(2)							X			
FMT_MTD.1(3)							X			
FMT_SMF.1							X			
FMT_SMR.1							X			
FPT_AMT.1							X			
FPT_ITT.1		X	X							X
FPT_RVM.1(1)										X
FPT_SEP.1(1)										X
FPT_STM.1							X		X	
FPT_TST.1							X			
FTA_TSE.1							X			

Table 13 TOE Security Requirement to TOE Security Objectives Mapping (continued)

	O.Authenticity	O.Confidentiality	O.Integrity	O.ID-Authentication	O.Key-Confidentiality	O.No-Replay	O.Secure-Operation	O.EAL	O.Audit-Record	O.Self-Protect
FTP_ITC.1	X	X	X		X	X				
FTP_RTC.1(EXP)							X			
ACM_AUT.1								X		
ACM_CAP.4								X		
ACM_SCP.2								X		
ADO_DEL.2								X		
ADO_IGS.1								X		
ADV_FSP.2								X		
ADV_HLD.2								X		
ADV_IMP.1								X		
ADV_LLD.1								X		
ADV_RCR.1								X		
ADV_SPM.1								X		
AGD_ADM.1								X		
AGD_USR.1								X		
ALC_DVS.1								X		
ALC_FLR.1								X		
ALC_LCD.1								X		
ALC_TAT.1								X		
ATE_COV.2								X		
ATE_DPT.1								X		
ATE_FUN.1								X		
ATE_IND.2								X		
AVA_MSU.2								X		
AVA_SOF.1								X		
AVA_VLA.1								X		

Table 14 TOE Requirements to TOE Security Objectives Rationale

Security Objective (TOE)	Security Requirement Rationale
O.Authenticity The TOE must provide the means for ensuring that a packet flow has been received from a trusted source.	The SFRs [FCO_NRO.2(1), FCO_NRO.2(2), FCS_COP.1(2), FCS_COP.1(4), FCS_COP.1(5), FDP_IFC.1(1), FDP_IFF.1(1), FDP_IFC.1(2), FDP_IFF.1(2), FTP_ITC.1] are sufficient to satisfy the objective because: • Packet flows received by the TOE must have been digitally signed using the FCO_NRO.2(1), FCO_NRO.2(2) SFRs with key material associated with an identified remote trusted IT product; • The FCS_COP.1(2) SFR is ensures that a message authentication code is generated and used therefore its authenticity can be established cryptographically; FCS_COP.1(4) and FCS_COP.1(5) support the protected communication with the CA to check that the digital certificate is trustworthy. • The IPSec and SSL information flow control SFPs and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(1) and FDP_IFC.1(2) SFRs; • The FDP_IFF.1(1) and FDP_IFF.1(2), SFRs are used to identify which TOE interfaces are authenticating which packet flow; and • The FTP_ITC.1 SFR establishes a trust relationship with another instance of the TOE to establish a LAN-LAN VPN; with an external authentication server, if configured, to authenticate users; and with a certificate authority, if configured, to obtain certificates.
O.Audit-Record The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times.	The SFRs [FAU_GEN.1, FAU_SAR.1, and FPT_STM.1] are sufficient to satisfy the objective because: FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event. FAU_GEN.1 depends on FPT_STM.1. It ensures that the date and time on the TOE are reliable. This is important for the audit trail. FAU_SAR.1 ensures the audit trail is presented in a human readable format.
O.Confidentiality The TOE must protect the confidentiality of packet flows transmitted to/from the TOE over an untrusted network.	The SFRs [FCS_COP.1(1), FDP_UCT.1(1), FDP_UCT.1(2), FMT_MSA.2(1), FDP_IFC.1(1), FDP_IFF.1(1), FDP_IFC.1(2), FDP_IFF.1(2), FTP_ITC.1, FPT_ITT.1] are sufficient to satisfy the objective because: • The FCS_COP.1(1) SFR ensures the confidentiality of transmissions through strong encryption; • The FDP_UCT.1(1) and FDP_UCT.1(2) SFR provides protection from disclosure of packet flows received by, or transmitted from the TOE over the external network; • FMT_MSA.2 ensures that the cryptographic values used for encryption are valid and not corrupted • The IPSec and SSL information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(1) and FDP_IFC.1(2) SFRs; • The FDP_IFF.1(1) and FDP_IFF.1(2), SFRs are used to identify which packet flow is to be protected when transmitted/received to/from the TOE; • The FTP_ITC.1 SFR establishes a trust relationship with a remote client; and • The FPT_ITT.1 SFR ensures the non-disclosure of TSF data transmitted between TOE components.

Table 14 TOE Requirements to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Requirement Rationale
O.Integrity The TOE must ensure that any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected.	The SFRs [FCS_COP.1(2), FDP_UIT.1(1), FDP_UIT.1(2), FMT_MSA.2(1), FDP_IFC.1(1), FDP_IFF.1(1), FDP_IFC.1(2), FDP_IFF.1(2); FTP_ITC.1, FTP_ITT.1] are sufficient to satisfy the objective because: • The FCS_COP.1(2) SFR ensures that a message authentication code is generated and used therefore its integrity can be established cryptographically; • The FDP_UIT.1(1) and FDP_UIT.1(2) SFRs provides integrity for packet flows received by, or transmitted from, the TOE; • FMT_MSA.2 ensures that the cryptographic values used for signatures are valid and not corrupted; • The IPSec and SSL information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(1) and FDP_IFC.1(2) SFRs; • The FDP_IFF.1(1) and FDP_IFF.1(2), SFRs are used to identify which packet flow is to be protected when transmitted/received to/from the TOE; • The FTP_ITC.1 SFR establishes a trust relationship with a remote client; and • The FPT_ITT.1 SFR ensures the integrity of TSF data transmitted between TOE components.
O.Key-Confidentiality The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt packet flows between the TOE and a remote client and when kept in short and long-term storage.	The SFRs [FCS_CKM.1 (1), FCS_CKM.1 (2), FCS_CKM.4(1), FMT_MSA.2(1), FDP_IFC.1(1), FDP_IFF.1(1), FDP_IFC.1(2), FDP_IFF.1(2), FTP_ITC.1] are sufficient to satisfy the objective because: • The FCS_CKM.1(1) and FCS_CKM.1(2) SFRs ensures that keys used for encryption and signatures are generated in accordance to specified algorithms and key sizes; • FCS_CKM.4 SFR ensures that keys can be safely destroyed; • FMT_MSA.2 ensures that cryptographic keys generated are checked to ensure they are not corrupted; • The IPSec and SSL information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(1) and FDP_IFC.1(2) SFRs; • The FDP_IFF.1(1) and FDP_IFF.1(2), SFRs are used to identify which packet flow is to be encrypted and decrypted when transmitted/received to/from the TOE; and • The FTP_ITC.1 SFR establishes a trust relationship with a remote client
O.ID-Authentication The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.	The SFRs [FIA_UAU.2, FIA_UAU.5(1), FIA_UID.2(1)] are sufficient to satisfy the objective because: • The FIA_UAU.2 ensures that all users are successfully authenticated before allowing any other TSF-mediated actions; • FIA_UAU.5(1) defines the authentication mechanisms that are supported by the TOE; • FIA_UAU.2 ensures that all users identify themselves before allowing any other TSF-mediated actions;

Table 14 TOE Requirements to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Requirement Rationale
O.No-Replay The TOE must provide a means to detect that a packet flow transmitted to the TOE has not been copied by an eavesdropper and re-transmitted to the TOE.	The SFRs [FCO_NRO.2(1), FCO_NRO.2(2), FDP_IFC.1(1), FDP_IFF.1(1), FDP_IFC.1(2), FDP_IFF.1(2), FTP_ITC.1] are sufficient to satisfy the objective because: • Packet flows received by the TOE are checked with sequence number that is uniquely associated with the remote client using the FCO_NRO.2(1), FCO_NRO.2(2) SFRs; • The IPSec and SSL information flow control SFPs and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(1) and FDP_IFC.1(2) SFRs; • The FDP_IFF.1(1) and FDP_IFF.1(2), SFRs are used to identify which packet flow is to be protected when transmitted/received to/from the TOE; and • The FTP_ITC.1 SFR establishes a trust relationship with a remote client.

Table 14 TOE Requirements to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Requirement Rationale
O.Secure-Operation The TOE must prevent unauthorized changes to its configuration.	The SFRs [FTA_TSE.1, FIA_UAU.2, FIA_UAU.5(1), FIA_UID.2(1), FAU_GEN.1, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.2(1), FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FPT_STM.1, FPT_AMT.1, FPT_TST.1, FCS_COP.1(3), FTP_RTC.1] are sufficient to satisfy the objective because: • The TSF can reject unauthorized session establishments by applying access control lists to deny session establishment, supported by FTA_TSE.1; • The FIA_UAU.2, and FIA_UAU.5(1) SFRs supports the requirement for multiple user authentication mechanisms before any actions are carried out on the TSF. The administrator must successful login thus only allowing authorized access to the TOE. FCS_COP.1(3) describes the encryption capability provided by SSH to allow an administrator to log in from a remote console; • The FIA_UID.2(1) SFR supports the requirement to identify the user before any actions are taken on that user's behalf; • The requirements for recording the occurrence of security relevant events that take place under TSF control is provided by FAU_GEN.1. FPT_STM.1 provides the timestamp for the audit records; • FMT_MOF.1(1) and FMT_MOF.1(2) ensures that only the administrator is permitted to change the configuration of information flows, operation of the TOE, authentication, and backup and restore TSF data, information flows, communication of the TOE with external ITE entities and audit trail data; • Only administrators can control the management of the security attributes by FMT_MSA.1(1), FMT_MSA.1(2); • Control over the assignment of the administrator role to different users is provided by FMT_SMR.1. No user will be able to assume the role of privileged administrator without explicitly requesting and being authenticated as having permission; • Control over the assignment of the VPN user role is provided by FMT_SMR.1. No user will be able to assume the VPN user role without successful authentication. • FMT_SMF.1 describes the security functions available to the administrators that can be used to ensure the secure operation of the TOE. • The requirement to restrict the ability to delete, clear, and load IPSec Pre-Shared Keys to administrators is provided by FMT_MTD.1(1); • The requirement to restrict the ability to change the default, clear, and specify IPSec and SSL configuration attributes to the administrator is provided by FMT_MTD.1(3); • The requirement to restrict the ability to modify, delete, and add user-oriented ACLs, user-oriented SSL attributes, and user and password identity credentials to the administrator is provided by FMT_MTD.1(2); • FPT_AMT.1 and FPT_TST.1 SFRs ensure that the TOE performs self-tests to verify the proper operation TOE; and • FTP_RTC.1 ensures that the remote administration is through a protected channel.

Table 14 TOE Requirements to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Requirement Rationale
O.EAL The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
O.Self-Protect The TOE must protect itself against attempts by unauthorized user to bypass, deactivate, or tamper with TOE security functions.	The SFRs [FPT_RVM.1(1), FPT_SEP.1(1), FPT_ITT.1] are sufficient to satisfy the objective because: • The FPT_RVM.1 SFR ensures that the TSF is always invoked from initial start-up and is non-bypassable; • The FPT_SEP.1 SFR ensures that the TSF has a domain of execution that is separate and cannot be violated by unauthorized users. This component also ensures that the domains of execution for the various processes are isolated and cannot be violated by unauthorized users; and • The FPT_ITT.1 SFR ensures TSF data is protected from disclosure and modification when distributed between TOE components.

Rationale for Security Functional Requirements of the IT Environment

Apart from OE.ID-Authentication and OE.Client, are the only security objectives for the environment that are IT in nature OE.Secure-Management is adminstrative in nature and is met by non-IT measures.

Table 15 IT Security Requirement to Environmental Objectives Mapping

	OE.ID-Authentication	OE.Client
FCS_CKM.1(3)		X
FCS_CKM.1(4)		X
FCS_CKM.4(2)		X
FCS_COP.1(6)		X
FCS_COP.1(7)		X
FIA_UAU.5(2)	X	
FIA_UID.2(2)	X	
FMT_MSA.2(2)		X
FPT_RVM.1(2)		X
FPT_SEP.1(2)		X

The following rationale is provided to support security functional requirements that are partially met within the TOE environment.

FCS_CKM.1(3), FCS_CKM.1(4), FCS_CKM.4(2), FCS_COP.1(6), FCS_COP.1(7), FMT_MSA.2(2)

These requirements are satisfied by the IT environment hosting the WebVPN. The WebVPN relies on the host operating system for SSL handshake and SSL encryption and decryption services. Those responsible for the TOE must ensure the IT environment hosting the Cisco WebVPN supports the same SSL protocol as the ASA. These requirements traces back to and aids in meeting the following objectives: OE.Client

FIA_UAU.5(2)

This component was chosen to ensure that multiple authentication mechanisms are used appropriately in all attempts to authenticate at the TOE from an internal or external network. This component traces back to and aids in meeting the following objective: OE.ID-Authentication.

Note that this requirement is partially satisfied by the TOE and partially by the TOE environment. Its presence under TOE environment security functional requirements is to address authentication by an external authentication server.

FIA_UID.2(2)

This component ensures that before anything occurs on behalf of a user, the user is identified to the TOE. This component traces back to and aids in meeting the following objective: OE.ID-Authentication.

FPT_RVM.1(2), FPT_SEP.1(2)

These requirements ensure the host IT environment for the VPN Client Components provide a protected execution domain and non-bypassability protection. These components traces back to and aids in meeting the following objective: OE.Client

TOE Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified TOE and IT Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. Table 16 lists the TOE Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale. Table 17 lists the IT Environment Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale.

N/A in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required. Satisfied in the Rationale column means the Security Functional Requirements dependency was included in the ST.

Table 16 TOE Security Functional Requirements Dependency Rationale

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FCO_NRO.2(1)	FCO_NRO.1	FIA_UID.1	Satisfied
FCO_NRO.2(2)	FCO_NRO.1	FIA_UID.1	Satisfied
FCS_CKM.1(1)	No other components.	FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	Satisfied
FCS_CKM.1(2)	No other components.	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	Satisfied

Table 16 TOE Security Functional Requirements Dependency Rationale (continued)

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FCS_CKM.4(1)	No other components.	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FMT_MSA.2	Satisfied
FCS_COP.1(1)	No other components.	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FMT_MSA.2	Satisfied
FCS_COP.1(2)	No other components.	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FMT_MSA.2	Satisfied
FCS_COP.1(3)	No other components.	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FMT_MSA.2	Satisfied
FCS_COP.1(4)	No other components.	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FMT_MSA.2	Satisfied
FCS_COP.1(5)	No other components.	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FMT_MSA.2	Satisfied
FDP_IFC.1(1)	No other components.	FDP_IFF.1	Satisfied
FDP_IFC.1(2)	No other components.	FDP_IFF.1	Satisfied
FDP_IFF.1(1)	No other components.	FDP_IFC.1, FMT_MSA.3	Satisfied
FDP_IFF.1(2)	No other components.	FDP_IFC.1, FMT_MSA.3	Satisfied
FDP_UCT.1(1)	No other components.	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	Satisfied
FDP_UCT.1(2)	No other components.	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	Satisfied
FDP_UIT.1(1)	No other components.	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	Satisfied
FDP_UIT.1(2)	No other components.	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	Satisfied
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied
FIA_UAU.5(1)	No other components.	No dependencies	N/A
FIA_UID.2(1)	FIA_UID.1	No dependencies	N/A
FMT_MOF.1(1)	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_MOF.1(2)	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_MSA.1 (1)	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_MSA.1 (2)	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_MSA.2(1)	No other components.	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	Satisfied
FMT_MSA.3	No other components.	FMT_MSA.1 FMT_SMR.1	Satisfied
FMT_MTD.1(1)	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_MTD.1(2)	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied

Table 16 TOE Security Functional Requirements Dependency Rationale (continued)

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FMT_MTD.1(3)	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_SMF.1	No other components.	No dependencies	N/A
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied
FPT_AMT.1	No other components.	No dependencies	N/A
FPT_ITT.1	No other components.	No dependencies	N/A
FPT_RVM.1(1)	No other components.	No dependencies	N/A
FPT_SEP.1(1)	No other components.	No dependencies	N/A
FPT_STM.1	No other components.	No dependencies	N/A
FPT_TST.1	No other components.	FPT_AMT.1	Satisfied
FTA_TSE.1	No other components.	No dependencies	N/A
FTP_ITC.1	No other components.	No dependencies	N/A
FTP_RTC.1(EXP)	No other components.	No dependencies	N/A

Table 17 IT Environment Security Functional Requirements Dependency Rationale

Security Functional Requirement (IT Environment)	Hierarchical To	Dependency	Rationale
FCS_CKM.1(3)	No other components.	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	Satisfied
FCS_CKM.1(4)	No other components.	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	Satisfied
FCS_CKM.4(2)	No other components.	[FDP_ITC.1 or FCS_CKM.1], FMT_MSA.2	Satisfied
FCS_COP.1(6)	No other components.	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Satisfied
FCS_COP.1(7)	No other components.	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Satisfied
FIA_UAU.5(2)	No other components.	No dependencies	N/A
FIA_UID.2(2)	No other components.	No dependencies	N/A
FMT_MSA.2(2)	No other components.	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	Satisfied
FPT_RVM.1(2)	No other components.	No dependencies	N/A
FPT_SEP.1(2)	No other components.	No dependencies	N/A

TOE Security Assurance Component Dependencies

This section of the ST demonstrates that the identified IT Security Assurance Requirements include the appropriate dependent SFRs. Table 18 lists the TOE Security Assurance Components and the Security Assurance Components each are dependent upon and any necessary rationale.

Table 18 EAL4 Augmented SAR Dependencies

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ACM_AUT.1	Partial CM automation	ACM_CAP.3	Yes
ACM_CAP.4	Generation support and acceptance procedures	ALC_DVS.1	Yes
ACM_SCP.2	Problem tracking CM coverage	ACM_CAP.3	Yes
ADO_DEL.2	Detection of modification	ACM_CAP.3	Yes
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1	Yes
ADV_FSP.2	Fully defined external interfaces	ADV_RCR.1	Yes
ADV_HLD.2	Security enforcing high-level design	ADV_FSP.1 ADV_RCR.1	Yes
ADV_IMP.1	Subset of the implementation of the TSF	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1	Yes
ADV_LLD.1	Descriptive low-level design	ADV_HLD.2 ADV_RCR.1	Yes
ADV_RCR.1	Informal correspondence demonstration	No dependencies	N/A
ADV_SPM.1	Informal TOE security policy model	ADV_FSP.1	Yes
AGD_ADM.1	Administrator guidance	ADV_FSP.1	Yes
AGD_USR.1	User Guidance	ADV_FSP.1	Yes
ALC_DVS.1	Identification of security measures	No dependencies	N/A
ALC_LCD.1	Developer defined life-cycle model	No dependencies	N/A
ALC_TAT.1	Well-defined development tools	ADV_IMP.1	Yes
ALC_FLR.1	Basic Flaw Remediation	No dependencies	N/A
ATE_COV.2	Analysis of Coverage	ADV_FSP.1 ATE_FUN.1	Yes
ATE_DPT.1	Testing: high-level design	ADV_HLD.1 ADV_FUN.1	Yes
ATE_FUN.1	Functional testing	No dependencies	N/A
ATE_IND.2	Independent testing – sample	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	Yes

Table 18 EAL4 Augmented SAR Dependencies (continued)

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
AVA_MSU.2	Validation of analysis	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	Yes
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1 ADV_HLD.1	Yes
AVA_VLA.2	Developer vulnerability analysis	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1 AGD_USR.1	Yes

Rationale for Strength of Function Claim

The rationale for the strength of function is based on a low attack potential. The security objective O.EAL states the TOE needs to be resistant to obvious penetration attacks which means the TOE should be resistant to penetration attacks performed by an attacker of low attack potential. The metric SOF-basic is an acceptable for low attack potential.

Rationale for TOE Assurance Requirements

The ST is written with EAL4 augmented with ALC_FLR.1.

EAL4 was chosen because it permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices. EAL4 provides the developers and users a moderate to high level of independently assured security in conventional commercial TOEs.

EAL4 is augmented by ALC_FLR.1 to help ensure that the customers can report the flaws and the flaws can be systematically corrected.

The chosen assurance level supports O.EAL, which is consistent with the postulated threat environment. The product will have undergone systematic vulnerability analysis by the developer and independent penetration testing by the evaluator.

Rationale for Explicitly Stated SFRs for the TOE

FTP_RTC.1 was created to correctly specify the TOE's use of a protected channel for remote administration. Per PD-0108, an explicit SFR based on FTP_ITC.1 is specified.

TOE Summary Specification Rationale

This section demonstrates the suitability of the security functions defined in the "TOE Security Functions" section on page 33 of meeting the TOE's Security Functional Requirements identified in the "TOE Security Functional Requirements" section on page 18 and that the security functional requirements are completely and accurately met by the TOE's Security Functions identified in the "TOE Security Functions" section on page 33.

Table 19 demonstrates the correspondence between the Security Functions and the TOE Security Functional Requirements. With the demonstration of correspondence given in Table 20, and the descriptions of the security functions given in the "TOE Security Functions" section on page 33on how the security functions are providing the functionality to meet the security functional requirements in Table 20 this provides the evidence of suitability of the security functions in meeting the security functional requirements stated in the "TOE Security Functional Requirements" section on page 18.

The mutually supportive nature of the IT security functions can be derived from the mutually support of the SFRs (demonstrated in the "Security Requirements Rationale" section on page 46), as each of the security functions can be mapped to one or more SFRs, as demonstrated in Table 19.

Table 19 TOE Security Functional Requirement to TOE Security Functions Mapping

TOE Security Functional Requirement	Security Management	Audit	IPSec VPN	SSL VPN	Identification and Authentication	Self-Protection	Clock
FAU_GEN.1		X					
FAU_SAR.1		X					
FCO_NRO.2(1)			X				
FCO_NRO.2(2)				X			
FCS_CKM.1(1)			X	X	X		
FCS_CKM.1(2)			X	X			
FCS_CKM.4(1)			X	X			
FCS_COP.1(1)			X	X			
FCS_COP.1(2)			X	X			
FCS_COP.1(3)					X		
FCS_COP.1(4)			X				
FCS_COP.1(5)			X				
FDP_IFC.1(1)			X				
FDP_IFC.1(2)				X			
FDP_IFF.1(1)			X			X	
FDP_IFF.1(2)				X		X	
FDP_UCT.1(1)			X				
FDP_UCT.1(2)				X			
FDP_UIT.1(1)			X				
FDP_UIT.1(2)				X			
FIA_UAU.2					X		
FIA_UAU.5(1)			X	X	X		
FIA_UID.2(1)					X		
FMT_MOF.1(1)	X						

Table 19 TOE Security Functional Requirement to TOE Security Functions Mapping (continued)

TOE Security Functional Requirement	Security Management	Audit	IPSec VPN	SSL VPN	Identification and Authentication	Self-Protection	Clock
FMT_MOF.1(2)	X						
FMT_MSA.1(1)	X						
FMT_MSA.1(2)	X						
FMT_MSA.2(1)	X						
FMT_MSA.3	X						
FMT_MTD.1(1)	X						
FMT_MTD.1(2)	X						
FMT_MTD.1(3)	X						
FMT_SMF.1	X						
FMT_SMR.1	X						
FPT_AMT.1						X	
FPT_ITT.1			X	X		X	
FPT_RVM.1(1)						X	
FPT_SEP.1(1)						X	
FPT_STM.1		X					X
FPT_TST.1						X	
FTA_TSE.1			X				
FTP_ITC.1			X		X		
FTP_RTC.1	X				X		

Table 20 Rationale of How the Security Functions Meet the Security Functional Requirements

SFR	SF and Rationale
FAU_GEN.1	Is implemented by the Audit Function. The Audit Function generates audit records for VPN related events with specific information captured for each event.
FAU_SAR.1	Is implemented by the Audit Function. The audit function provides the administrator with the ability to read audit records which are stored locally on the TOE. These audit records are presented in human readable form.
FCO_NRO.2(1)	Is implemented by the IPSec VPN Function. The IPSec VPN Function uses digital signatures and signing algorithms to guarantee the identity of SA peers. To create an IPSec session, the IPSec VPN Function and the VPN Client must determine exactly which algorithms to use for encryption and integrity. The security association is the method used by the IPSec VPN Function uses to track all the particulars concerning a given IPSec session. The SA uniquely identifies a unidirectional VPN connection.

Table 20 Rationale of How the Security Functions Meet the Security Functional Requirements (continued)

SFR	SF and Rationale
FCO_NRO.2(2)	Is implemented by the SSL VPN Function. The SSL VPN Function uses digital signatures and signing algorithms to guarantee the identity of the client. To create an SSL session, the SSL VPN Function and the client must negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data being sent. Each SSL session is defined by SSL related parameters that includes peer certificates, MAC secret keys, and write keys for data encryption/decryption.
FCS_CKM.1(1)	Is implemented by the IPSec VPN Function, SSL VPN Function, and Identification and Authentication Function. The IPSec VPN and SSL VPN functions use an RSA algorithm to generate keys used for bulk encryption. The Authentication Function uses RSA generated keys to encrypt remote administrator sessions.
FCS_CKM.1(2)	Is implemented by IPSec VPN Function and SSL VPN Function. Both functions use Diffie-Hellman generated keys for bulk encryption.
FCS_CKM.4(1)	Is implemented by IPSec VPN Function and SSL VPN Function. Both functions contain a method for overwriting (destroying) cryptographic keys which the TOE creates.
FCS_COP.1(1)	Is implemented by IPSec VPN Function and SSL VPN Function. Both functions implement bulk encryption and decryption in accordance with triple DES or AES on transmitted packets.
FCS_COP.1(2)	Is implemented by IPSec VPN Function and SSL VPN Function. Both functions provide a method by which a message authentication code is generated and used to provide integrity and authenticity protection .
FCS_COP.1(3)	Is implemented by the Identification and Authentication Function. The Identification and Authentication Function provides a protected interface for remote administration such that the connection is encrypted using SSH.
FCS_COP.1(4)	Is implemented by the IPSec VPN Function by providing the cryptographic mechanism for signing that supports the retrieval of digital certificates from a Certificate Authority (CA) using the Simple Certificate Enrollment Protocol (SCEP)..
FCS_COP.1(5)	Is implemented by the IPSec VPN Function by providing the cryptographic mechanism for encryption/ decryption that supports the retrieval of digital certificates from a Certificate Authority (CA) using the Simple Certificate Enrollment Protocol (SCEP).
FDP_IFC.1(1)	Is implemented by the IPSec VPN Function. The IPSec VPN Function examines request to establish an IPSec VPN and once a pair of SAs is created for the VPN session, decrypts and encrypts packets..
FDP_IFC.1(2)	Is implemented by the SSL VPN Function. The SSL VPN Function examines requests to establish an SSL VPN and once an SSL is established, permits or denies traffic for the SSL session.
FDP_IFF.1(1)	Is implemented by the IPSec VPN Function and Self-Protection Function. The IPSec VPN Function examines request to establish an IPSec VPN and applies the information flow rules to establish a VPN with a successfully authenticated client. The Self-Protection Function ensures all packets through the TOE are subject to inbound packet filtering rules
FDP_IFF.1(2)	Is implemented by the SSL VPN Function and Self-Protection Function. The SSL VPN Function examines request to establish a SSL VPN and applies the information flow rules to establish a VPN with a successfully authenticated client. The Self-Protection Function ensures all packets through the TOE are subject to inbound packet filtering rules
FDP_UCT.1(1)	Is implemented by the IPSec VPN Function. The IPSec VPN function provides ESP which encrypts an IP datagram providing confidentiality
FDP_UCT.1(2)	Is implemented by the SSL VPN Function. The SSL VPN Function provides confidentiality for SSL connections by encrypting the application data as part of the SSL Record protocol.
FDP_UIT.1(1)	Is implemented by the IPSec VPN Function. The IPSec VPN Function provides ESP which signs an IP datagram providing integrity.

Table 20 Rationale of How the Security Functions Meet the Security Functional Requirements (continued)

SFR	SF and Rationale
FDP_UIT.1(2)	Is implemented by the SSL VPN Function. The SSL VPN Function uses a MAC to provide message integrity. A MAC is computed by using a shared secret key and message content and computing a hash value.
FIA_UAU.2	Is implemented by the Identification and Authentication Function. The Identification and Authentication Function requires users to undergo authentication before access to its management interfaces is granted.
FIA_UAU.5(1)	Is implemented by the SSL VPN Function, IPSec VPN Function and Identification and Authentication Function. The Identification and Authentication Function provides the I&A interface to be used for authenticating remote VPN users and administrators.
FIA_UID.2(1)	Is implemented by the Identification and Authentication Function. The Identification and Authentication Function requires users to undergo identification before access to its management interfaces is granted.
FMT_MOF.1(1)	.Is implemented by the Security Management Function. The Security Management Function permits only the authorized administrator to perform the following functions enable, disable VPN operation of the TOE, user of the external authentication server; and use of the a certificate authority server.
FMT_MOF.1(2)	Is implemented by the Security Management Function. The Security Management Function permits only the authorized administrator to perform the following functions: implement IPSec information flow control SFP, implement SSL information flow control SFP, backup and restore of TSF data, information flow rules audit trail data; and control communication of authorized external IT entities.
FMT_MSA.1 (1)	Is implemented by the Security Management Function. The Security Management Function permits the authorized administrator to modify and delete security attributes in the information flow rules that implement the IPSec information flow control SFP.
FMT_MSA.1 (2)	Is implemented by the Security Management Function. The Security Management Function permits the authorized administrator to modify and delete security attributes in the information flow rules that implement the SSL information flow control SFP.
FMT_MSA.2(1)	Is implemented by the Security Management Function. The Security Management Function validates all cryptographic attributes that a successfully authenticated administrator may input. Also, all cryptographic attributes are checked to ensure that they are not corrupted.
FMT_MSA.3	Is implemented by the Security Management Function. The Security Management Function ensures the restrictive default values are allocated to security attributes for the IPSec information flow control SFP and SSL information flow control SFP, and allowing the authorized administrators to alter the default values.
FMT_MTD.1(1)	Is implemented by the Security Management Function. The Security Management Function only permits the authorized administrator to alter the Pre-Shared Keys. The Pre-Shared Keys are used by the IPSec VPN Function during the IKE negotiation.
FMT_MTD.1(2)	Is implemented by the Security Management Function. The Security Management Function only permits the authorized administrator to configure user-oriented SSL attributes and user and password identity credentials. The SSL attributes are assigned to groups and define what applications and urls are permitted for a user, and user/passwords are used to authenticate users.
FMT_MTD.1(3)	Is implemented by the Security Management Function. The Security Management Function only permits the authorized administrator to configure IPSec configuration attributes and SSL configuration attributes. These attributes are used by the IPSec VPN Function and SSL VPN Function.

Table 20 Rationale of How the Security Functions Meet the Security Functional Requirements (continued)

SFR	SF and Rationale
FMT_SMF.1	Is implemented by the Security Management Function. The Security Management Function provides the security management functions to enable or disable the VPN operation of the TOE; enable or disable the external authentication function; enable or disable the use of a certificate authority server; enable, disable, determine and modify the behavior of the functions that implement the IPSec information flow control SFP; enable, disable, determine and modify the behavior of the functions that implement the SSL information flow control SFP; enable, disable, determine and modify the behavior of the backup and restore function for TSF data, information flow rules, and audit trail data; enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE; modify and delete the information flow rules for IPSec VPN and SSL VPN; and load, delete, and clear IPSec Pre-Shared Keys; modify, delete, and add user-oriented SSL attributes, and user and password identity credentials; change_default, clear, and specify IPSec configuration attributes and SSL configuration attributes; and read audit records.
FMT_SMR.1	Is implemented by the Security Management Function. The Security Management Function maintains the VPN user and authorized administrator role and ensures that a user is authenticated before allowing them to perform functions only provided for the authorized administrator and VPN user.
FPT_AMT.1	Is implemented by the Self-Protection Function. The Self-Protection Function initiates a suite of test upon startup to ensure proper operation of the underlying abstract machine.
FPT_ITT.1	Is implemented by the Self-Protection Function, IPSec VPN Function and SSL VPN Function. All VPN connections are protected between the ASA and the WebVPN and ASA and Cisco VPN Client.
FPT_RVM.1(1)	Is implemented by the Self-Protection Function. The TOE makes sure that security enforcing functions are invoked and succeed before allowing any other mediated action to occur.
FPT_SEP.1(1)	Is implemented by the Self-Protection Function. The Self-Protection Function provides a separation of information streams traversing the TOE. The TOE is a dedicated device, with no general purpose operating system, disk storage, or programming interface. No untrusted processes are permitted on the TOE.
FPT_STM.1	Is implemented by the Clock Function and used by the Audit Function. The Clock Function provides the Audit Function with the time stamps. The Audit function uses the time stamp to record the date and time in an audit record.
FPT_TST.1	Is implemented by the Self-Protection Function. The Self-Protection Function initiates a suite of tests upon startup to ensure proper operation of the TOE functions.
FTA_TSE.1	Is implemented by IPSec VPN Function and SSL VPN Function. These functions examine each packet and discard those which do no match the interface access control list associated with it.

Table 20 Rationale of How the Security Functions Meet the Security Functional Requirements (continued)

SFR	SF and Rationale
FTP_ITC.1	Is implemented by the IPSec VPN Function and Identification and Authentication Function. The IPSec VPN Function authenticates IPSec peers using pre-shared keys, or digital certificates and establishes a trusted channel (called Security Associations) for the communication of information with assured identification of end-points; using ESP on IP datagrams to provide confidentiality, authentication, integrity and non-repudiation of sender; and maintains a cryptographic map which ensures that packet flow source, destination and transmission parameters are controlled. The IPSec VPN Function uses SCEP protected communications to interface with a Certificate Authority Server. Identification and Authentication Function satisfy this requirement by requiring the remote VPN Client user to undergo authentication before a VPN tunnel is established or requiring the administrator to authenticate before performing any TSF-mediated actions. This requirement ensures that the TOE uses a trusted source external authentication server to provide authentication services if configured by the administrator.
FTP_RTC.1	Is implemented by the Security Management Function and Identification and Authentication Function by ensuring a protected channel is provided for remote administration. The protected channel requires the use of SSH.

Appendix A: TOE Equivalency

All of the hardware in the TOE belong to the same Cisco ASA 5500 hardware family of products based on the same hardware platform (circuit board, CPU family). The differences are amount of RAM, processor speed, and on-board network interface cards. All the devices execute the same 7.2(4)18 software image.

The following table demonstrates the performance differences between the different ASA models.

Features	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
Market	SMB, Branch Office	SMB	Enterprise	Large Enterprise	Large Enterprise
CPU	500 MHz AMD GX3	1.6 GHz Celeron	2.0 GHz Celeron	2.0 GHz Pentium 4	3 .0 GHz Pentium 4
Maximum Firewall Throughput (Mbps)	150	300	450	650	1.2 Gbps
Maximum Firewall Connections	10,000	50,000	280,000	400,000	650,000
Maximum Firewall Connections/Second	4,000	9,000	12,000	25,000	36,000
Memory (MB)	256	256	512	1 GB	4 GB
System Flash (MB)	64	64	64	64	64
Integrated Ports	8 port 10/100 switch with 2 Power over Ethernet ports	2-10/100/1000, 3-10/100	4-10/100/1000, 1-10/100	4-10/100/1000, 1-10/100	8-10/100/1000, 4-SFP, 1-10/100
Maximum Virtual Interfaces (VLANs)	20	50	150	200	250
Application Layer Security	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewalling	Yes	Yes	Yes	Yes	Yes
Security Contexts (Included/Maximum) 3	0/0	0/0	2/20	2/50	2/50

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html