Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform Security Target

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform solutions. 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.

Version 1.0
July 2011

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

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

Table of Contents

List of Tables

List of Figures

Security Target Introduction

The Security Target contains the following sections:

- Security Target Introduction
- TOE Description
- Conformance Claims
- Security Problem Definition
- Security Objectives
- Security Requirements
- TOE Summary Specification 49
- Rationale

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 Basic Robustness.

Table 1 ST and TOE Identification

ST Title	Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform Security Target
ST Version	1.0
Publication Date	July 2011
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platforms, Cisco AnyConnect, Cisco VPN Client, Cisco SSL VPN (clientless), Cisco Adaptive Security Device Manager (ASDM)
TOE Hardware Models	Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20, and 5580-40
TOE Software Version	Cisco ASA Release 8.3.2, Cisco AnyConnect Release 2.5, Cisco VPN Client Release 5.0, Cisco Adaptive Security Device Manager (ASDM) 6.3.2
Keywords	Firewall, VPN, Encryption, Data Protection, Authentication

TOE Overview

The TOE is a purpose-built security platform that combines application-aware firewall and VPN services for small and medium-sized business (SMB) and enterprise applications.

TOE Product Type

The TOE consists of hardware and software used to construct Virtual Private Networks (VPNs) and Firewall solutions.

For firewall services, the ASA 5500 Series provides application-aware stateful packet filtering firewalls. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator for firewalls. This header information includes source and destination host (IP) addresses, source and destination port numbers, and the transport service application protocol (TSAP) held within the data field of the IP packet. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated.

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

The application-inspection capabilities automate the network to treat traffic according to detailed policies based not only on port, state, and addressing information, but also on application information buried deep within the packet header. By comparing this deep-packet inspection information with corporate policies, the firewall will allow or block certain traffic. For example, it will automatically drop application traffic attempting to gain entry to the network through an open port-even if it appears to be legitimate at the user and connection levels-if a business's corporate policy prohibits that application type from being on the network.

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), Cisco Clientless SSL VPN, network-aware site-to-site VPN connectivity, and Cisco AnyConnect VPN client. IPSec provides confidentiality, authenticity, and integrity for IP data transmitted between trusted (private) networks over untrusted (public) links or networks. SSL VPN uses a Web browser and SSL encryption to secure connections between remote users and specific, supported internal protected resources. AnyConnect uses the Datagram Transport Layer Security (DTLS) and Secure Socket Layer (SSL) protocols to provide remote users with secure VPN connections to the ASA. Note: these VPN configurations are only supported in Routed Single Context Mode.

For management purposes, the ASDM is included. ASDM allows the ASA to be managed from a graphical user interface. Its features include:

- Rapid Configuration: in-line and drag-and-drop policy editing, auto complete, configuration wizards, appliance software upgrades, and online help;
- Powerful Diagnostics: Packet Tracer, log-policy correlation, packet capture, regular expression tester, and embedded log reference;
- Real-Time Monitoring: device, firewall, content security, real-time graphing; and tabulated metrics;
- Management Flexibility: A lightweight and secure design enables remote management of multiple security appliances.

Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 2 ST and TOE Identification

Operational Environment Component	Required	Usage/ Purpose Description for TOE performance
VPN Peer	No	This includes any peer with which the TOE participates in VPN communications. VPN peers may be any device that supports IPSec communications. Both VPN clients and VPN gateways are considered VPN peers by the TOE. Note that there are two VPN clients that are considered part of the TOE, and they are not included in this category.
VPN Client Platform	Yes	This includes the platform and OS for both the Cisco AnyConnect Release 2.5 and Cisco VPN Client Release 5.0. • The AnyConnect 2.5 client operates on any of the following OSs: • Windows 2000, including Service Pack 1, 2, 3, and 4 • Windows XP 32-bit (x86) and 64-bit (x64), including Service Pack 1, 2, and 3 • Windows Vista 32-bit (x86) and 64-bit (x64), including Service Pack 1 and 2 (SP1/SP2) • Windows 7 32-bit (x86) and 64-bit (x64) • Mac OS X Power PC and Intel 10.4 and 10.5 • Linux Intel (any 2.6.x kernel OS) The VPN Client 5.0 operates on any of the following OSs: • Microsoft Windows XP, including Service Pack 1, 2, and 3 • Windows 2000, including Service Pack 1, 2, 3, and 4 or • Windows Vista platform including Service Pack 1 and 2 (SP1/SP2)
ASDM Management	Yes	The ASDM 6.3.2 operates from any of the

Operational Environment Component	Required	Usage/ Purpose Description for TOE performance
Platform		following operating systems: • Microsoft Windows XP, including Service Pack 1, 2, and 3 • Windows Vista, including Service Pack 1 and 2 (SP1/SP2) • Windows 2003 Server, including Service Pack 1 and 2 and • MacOS X Note that that ASDM software is installed on the ASA appliance and the management platform is used to connect to the ASA and run the ASDM. The only software installed on the management platform is a Cisco ASDM Launcher.
Webrowser	No	The following webbrowers are supported for access to the ASDM; • Internet Explorer (6.0 or higher) • Firefox (1.5 or higher) • Safari (2.0 or higher)
Remote Authentication Server	Yes	A RADIUS or TACACS+ server is required for use with the TOE.
NTP Server	No	The TOE supports communications with an NTP server. A solution must be used that supports MD5 hashing of communications with up to a 32 character key.
Peer Certificate Authority (CA)	No	The TOE supports OCSP communication with other CAs.
Syslog Server	Yes	A syslog server with the capability to support SSL-protected TCP syslog communications is required for use with the TOE.

TOE Description

Figure 1: ASA Appliances

This section provides an overview of the Cisco ASA Firewall and VPN Platforms Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE consists of a number of components including:

- One or more 5500 Appliances: The appliance is a single-use device with a hardened version of the Linux Kernel 2.6 (32 bit for everything but the 5580s and 64 bit for the 5580s) running ASA Release 8.3.2. Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540, ASA-5550, ASA-5580-20, and 5580-40 each with the following processor and interface configurations:

  - 5505 – 500 MHz AMD GX3 – Eight 10/100 copper Ethernet ports;
  - 5510 – 1.6 GHz Celeron – Five 10/100 copper Ethernet ports (two can be 10/100/1000 copper Ethernet ports), one out-of-band management port;
  - 5520 – 2.0 GHz Celeron – Four 10/100/1000 copper Ethernet ports, one out-of-band management port;
  - 5540 – 2.0 GHz Pentium 4 – Four 10/100/1000 copper Ethernet ports, one out-of-band management port;
  - 5550 – 3.0 GHz Pentium 4 – Eight Gigabit Ethernet ports, four small form factor-pluggable (SFP) fiber ports, one Fast Ethernet port;
  - 5580-20 – Four 2.6GHz AMD Opteron – Two RJ-45 management ports, two Gigabit Ethernet management ports, with space for 6 interface expansion cards:
    - Up to twelve 10Gigabit Ethernet (10GE) ports (two per ASA5580-2X10GE-SR card)
    - Up to twenty-four Gigabit Ethernet ports (four per ASA5580-4GE-FI card)
    - Up to twenty-four 10/100/1000 Ethernet ports (four per ASA5580-4GE-CU card)
  - 5580-40 – Four 2.6GHz AMD Opteron – Two RJ-45 management ports, two Gigabit Ethernet management ports, with space for 6 interface expansion cards:
    - Up to twelve 10Gigabit Ethernet (10GE) ports (two per ASA5580-2X10GE-SR card)
    - Up to twenty-four Gigabit Ethernet ports (four per ASA5580-4GE-FI card)
    - Up to twenty-four 10/100/1000 Ethernet ports (four per ASA5580-4GE-CU card)

- VPN clients: The following VPN clients are included with the TOE.

- Cisco AnyConnect Release 2.5 (including Cisco SSL VPN Clientless software)
- Cisco VPN Client Release 5.0
  - ASDM software: The ASDM 6.3.2 software is installed on the ASA server. Only the Cisco ASDM Launcher is installed locally on the management platform. The ASDM software can also be launched by connecting to the https port on the ASA

Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the Cisco ASA Firewall and VPN Platforms solution. The TOE is comprised of the following:

Table 3 Physical Scope of the TOE

TOE Configuration	Hardware Configurations	Software Version
ASA 5505 	The Cisco ASA 5505 features a flexible 8-port 10/100 Fast Ethernet switch, whose ports can be dynamically grouped to create up to three separate VLANs for home, business, and Internet traffic for improved network segmentation and security.	ASA release 8.3.2, including a Linux Kernel 2.6
ASA 5510 	The Cisco ASA 5510 Adaptive Security Appliance provides high-performance firewall and VPN services and five integrated 10/100 Fast Ethernet interfaces (2 can be 10/100/1000) and support for up to 100 VLANs.	ASA release 8.3.2, including a Linux Kernel 2.6
ASA 5520 	The Cisco ASA 5520 Adaptive Security Appliance provides high-performance firewall and VPN services and four Gigabit Ethernet interfaces and support for up to 150 VLANs.	ASA release 8.3.2, including a Linux Kernel 2.6
ASA 5540 	The Cisco ASA 5540 Adaptive Security Appliance provides high-performance firewall and VPN services and four Gigabit Ethernet interfaces and support for up to 200 VLANs.	ASA release 8.3.2, including a Linux Kernel 2.6
ASA 5550 	The Cisco ASA 5540 Adaptive Security Appliance provides high-performance	ASA release 8.3.2, including a Linux Kernel 2.6

	firewall and VPN services via eight Gigabit Ethernet interfaces, four Small Form-Factor Pluggable (SFP) fiber interfaces, and support for up to 250 VLANs.	
ASA 5580-20 **ASA 5580-40** 	The Cisco ASA 5580 Adaptive Security Appliances provide six interface expansion card slots with support for up to 24 Gigabit Ethernet interfaces or up to 12 10Gigabit Ethernet interfaces or up to twenty-four 10/100/1000 Ethernet ports, and support for up to 250 VLANs.	ASA release 8.3.2, including a Linux Kernel 2.6
Cisco AnyConnect (including Cisco SSL VPN Clientless software)	Not applicable	Release 2.5
Cisco VPN Client	Not applicable	5.0
ASDM 6.3.2	Not applicable	Release 6.3.2

Logical Scope of the TOE

The TOE is comprised of several security features. The following security features are defined in more detail below.

1. VPN and/or Firewall Information Flow Control
2. Audit
3. Identification & Authentication
4. Management
5. Cryptography

These features are described in more detail in the subsections below.

VPN and/or Firewall Information Flow Control

The Information Control functionality of the TOE allows authorized administrators to set up rules between interfaces of the TOE. These rules control whether a packet is transferred from one interface to another and/or transferred encrypted based upon:

1. User identities (source and/or destination)
2. Presumed address of source subject
3. Presumed address of destination subject
4. Service used
5. Transport layer protocol

6. Security-relevant service command
7. Network interface on which the connection request occurs and is to depart

Packets will be dropped unless a specific rule or policy in an access control list (ACL) has been set up to allow the packet to pass. The order of Access Control Entries (ACEs) in an ACL 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.

In providing the Information Flow Control functionality, the TOE has the ability to translate network addresses contain within a packet, called Network Address Translation. Depending upon the TOE configuration the address can be translated into a permanently defined static address, an address selected from a range or into a single address with a unique port number (Port Address Translation). Also Network Address Translation can be disabled, so that addresses are not changed when passing through the TOE.

The TOE has the ability to reject requests in which the subject specifies the route in which information flows en route to the receiving subject. Through use of protocol filtering proxies, the TOE can also reject Telnet or FTP command requests that do not conform to generally accepted, published protocol definitions.

IPSec VPN

The IPSec VPN Function includes 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.

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.

SSL VPN

SSL VPN connectivity is provided through a clientless solution and a client solution – AnyConnect. The clientless SSL VPN, which is actually branded as SSL VPN, uses the SSL (v3.1) protocol and its successor, Transport Layer Security (TLS) v1.0 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. 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.
- Administrator enabling clientless SSL VPN sessions on the TOE interface that remote users connect to with the 'svc enable' command.

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).

The user is prompted to enter a username and password. If configured, the user can be authenticated using a digital certificate. A remote 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 SSL VPN connection. The clientless connection 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

The AnyConnect client provides remote end users running Microsoft Windows Vista, Windows 7, Windows XP or Windows 2000, Linux, or Macintosh OS X, with a Cisco SSL VPN client, and supports applications and functions that are unavailable to a clientless, browser-based SSL VPN connection. The same client version is used for all of the various OS platforms. In addition, the AnyConnect client supports connecting to IPv6 resources over an IPv4 network tunnel. AnyConnect utilizes the SSL v3.1 and DTLS v1.0 protocol. DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP, and it is specified in RFC 4347. DTLS allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. If DTLS is not enabled, SSL VPN connections connect with an SSL VPN tunnel only.

The client is configured by the authorized administrator on the ASA and can be automatically downloaded to remote users when they log in, or it can be manually installed as an application on PCs by a network administrator. After downloading, it can automatically uninstall itself after the connection terminates, or it can remain on the remote PC for future SSL VPN connections.

Authentication of AnyConnect users can be done via user ID and reusable password, or via digital certificates.

Single or Multiple Context

A security context is a collection of processes that exist to model the logical virtual firewall into the constraints of the hardware. Each security context (virtual device) is treated as a separate independent device with its own security policy, interfaces, administrators, and configuration file.

When the firewall is operating in single routed mode one instance of a security context is present and executing. When the firewall is configured in multiple-context mode multiple security contexts are executing simultaneously. Each context in multiple-context mode is made up of the same processes used in single routed mode, but a process establishes the “context” for a request and then sets its operating variables to use the control/data memory owned by the context. There is no difference between the processes that are running for a single instance of a context in single, routed mode or multiple-context mode. Multiple contexts are similar to having multiple stand-alone devices.

The ASA 5505 does not support multiple contexts. Its only separation support is creation of up to 20 VLANs on its eight switch ports. The other platforms also support VLANs (up to the amounts indicated in *Table 3*).

Routed or Transparent Mode

The security appliance can run in these two firewall modes:

- Routed mode
- Transparent mode

In routed mode, the security appliance is considered to be a router hop in the network. It can perform NAT between connected networks, and can use OSPF or passive RIP (in single context mode). Routed mode supports many interfaces. Each interface is on a different subnet. Interfaces can be shared between contexts. Note that IPv6 is only supported in Routed mode.

In transparent mode, the security appliance acts like a "bump in the wire," or a "stealth firewall," and is not a router hop. The security appliance connects the same network on its inside and outside interfaces. No dynamic routing protocols or NAT are used. However, like routed mode, transparent mode also requires access lists to allow any traffic through the security appliance, except for ARP packets, which are allowed automatically. Transparent mode can allow certain types of traffic in an access list that is blocked by routed mode, including unsupported routing protocols. Transparent mode can also optionally use EtherType access lists to allow non-IP traffic. Transparent mode only supports two interfaces, an inside interface and an outside interface, in addition to a dedicated management interface, depending on the platform (all but the 5505).

NOTE: The TOE must run in Routed Single Context mode only when configured to perform VPN transmissions.

Audit

The TOE’s Audit security function supports audit record generation and review. The TOE provides date and time information that is used in audit timestamps. The events generated by the TOE include all commands executed by the authorized administrator, in addition to cryptographic operations, traffic decisions, indication of the logging starting and stopping and other system events.

The local buffer on the ASA stores the audit records, and its size is configurable by the authorized administrator. The same protection is given to these stored events that is given to all system files on the ASA. Access to them is restricted only to the authorized administrator, who has no access to edit them, only to copy or delete (clear) them.

The audit records can be viewed either locally or remotely (via SSH v2) on the ASA CLI or through a Real-Time Log Viewer in ASDM (secured via HTTPS tunnel). The Real-Time Log Viewer in ASDM

allows for filtering of events or searches by keyword and for sorting of events by the header fields in the event viewer. This allows an authorized administrator to quickly locate the information that they are looking for and quickly detect issues. This log viewer needs to be open and active during TOE operation in order to display the records as they are received.

When the buffer on the ASA reaches its capacity, the administrator will be notified that this has occurred via an alert log entry, and in order to minimize the number of events lost, new sessions through the ASA will be temporarily stopped. This will give the administrator the time to offload the audit events to another server. This can be done directly from the Real-Time Log Viewer on ASDM, where functionality is given to save the events to a local file on the host machine for backup.

Identification & Authentication

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. 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 at the CLI or screens in ASDM. The TOE can be configured to use an external authentication server for single-use authentication 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.

A lockout mechanism is enforced after an administrator-specified number of failed attempts. This functionality is enforced for all locally authenticated users. The lockout results in the user being unable to authenticate until an authorized administrator unlocks the account.

VPN users are authenticated through their client (or through SSL session if clientless) to the TOE via a reusable password mechanism. If enabled, certificate-based authentication is used for clientless SSL VPN.

Management

The Management functionality permits an authorized administrator from a physically secure local connection, an SSHv2 encrypted connection (the encryption is subject to FIPS PUB 140-2 security functional requirements) or an HTTPS-tunneled ASDM connection from an internal trusted host or a remote connected network to perform the following actions:

1. Enable or disable the operation of the TOE.
2. Enable or disable the multiple use authentication functions.
3. Enable, disable, determine and modify the behavior of the audit trail management.
4. Enable, disable, determine and modify the behavior of the functionality to backup and restore TSF data, information flow rules, and audit trail data.
5. Enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE.
6. Delete and create attributes/ rules for VPN and information flow.
7. Delete attributes from a rule, modify attributes in a rule, add attributes to a rule.
8. Query, modify, delete, and assign the user attributes.
9. Set the time and date used to form the timestamps.
10. Specify the limits for the number of authentication failures.

All of these management functions are restricted to the authorized administrator of the TOE. The authorized administrator is defined as having the full set of privileges on the ASA, which is indicated by a level 15 privilege on a scale from 0 to 15.

All local user credentials on the ASA are stored in a central database. The users are differentiated as ASA administrators, VPN users, or cut-through proxy users (users required to be authenticated before sessions through the ASA are allowed) through a service-type attribute and by privilege level. Only ASA administrators have any local privileges on the ASA.

Note that the VPN user role is not an administrative role, and its only purpose is to establish VPN connections to or through the TOE. It has no other privileges with respect to the TOE.

Cryptography

The TOE relies on FIPS PUB 140-2 validation for testing of cryptographic functions. The FIPS certificate is 1436 for ASA and the clients are FIPS compliant as determined by testing by SAIC.

The Cisco VPN Client uses cryptography at two abstraction levels:

1. User space: Here cryptography is used for IKE. Once the IKE exchange is completed the keys are plumbed down to the kernel space. For supporting IKE, the module utilizes AES, Triple-DES, HMAC-SHA-1, SHA-1, RSA (digital signatures), RSA (encrypt/decrypt), and Diffie-Hellman. These algorithms are provided by RSA Crypto-C Micro Edition dynamic library.
2. Kernel space: At this level, cryptography is used for bulk IPSec encryption/decryption and MACing. To support this, the module uses AES, Triple-DES, SHA-1 and HMAC-SHA-1 algorithms. These algorithms are provided by RSA BSAFE Crypto-Kernel library.

The Cisco AnyConnect client uses cryptography at two junctures:

1. Session setup: Here cryptography is used as part of the protocol used to set-up HTTPS sessions using TLS.
2. Data protection: Once the session set-up is complete, cryptography is used to protect data that traverses over the TLS and DTLS tunnels.

Unlike session set-up, all crypto for data protection is offloaded to the openSSL library on Windows, Linux as well as MAC OS platforms. To ensure that openSSL utilizes only FIPS approved crypto algorithms, the client has a policy file (called AnyConnectLocalPolicy) where FIPS mode can be set.

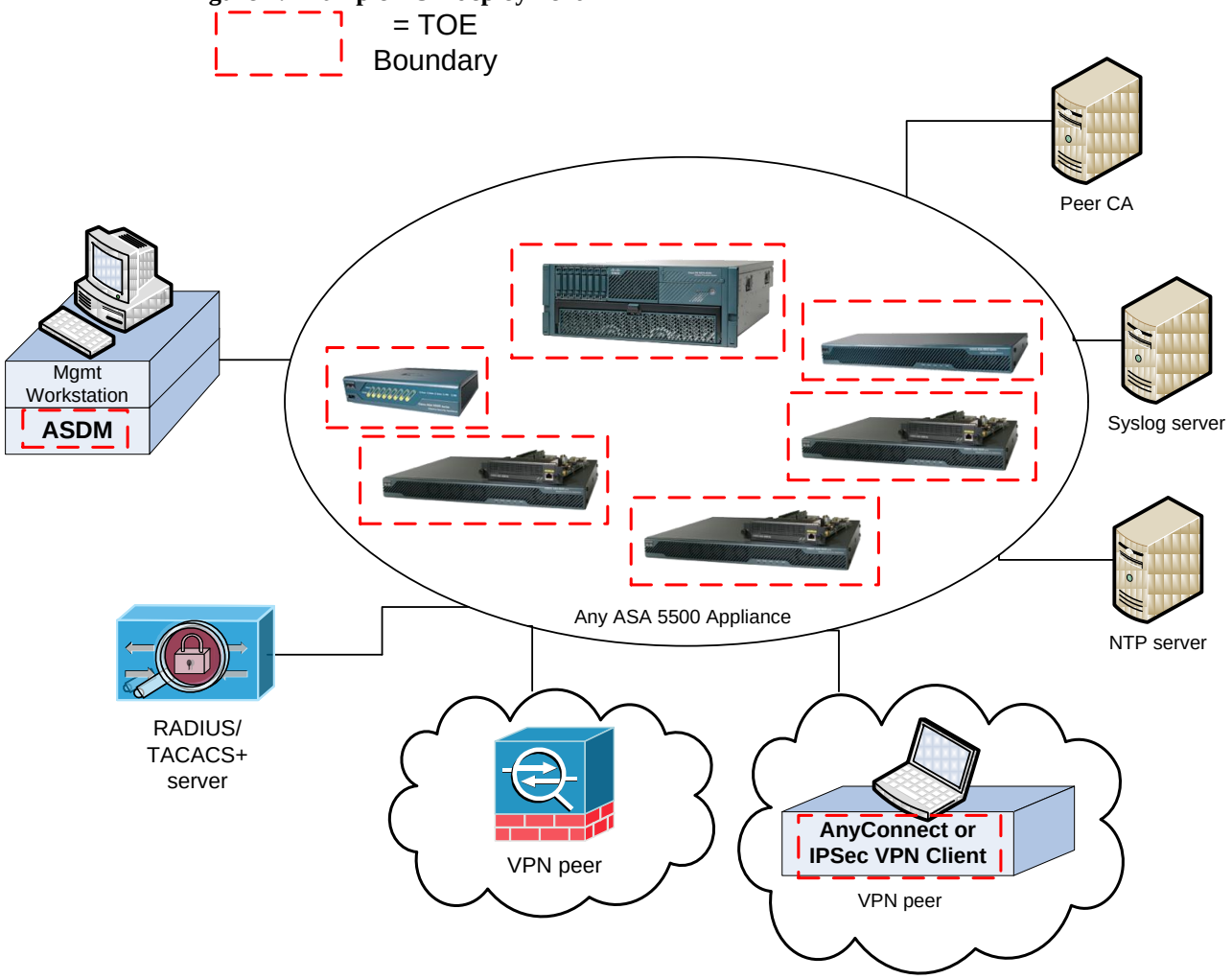
The ASA uses cryptography in the following forms:

1. Identity certificates for the ASA itself, and also for use in IPSEC, TLS, and SSH negotiations. This is provided by RSA keys.
2. Key agreement for IKE, TLS, and SSH sessions. This is provided by Diffie-Hellman.
3. For TLS traffic keys, SSH session keys, IPSec authentication keys, IPSec traffic keys, IKE authentication keys, IKE encryption keys, and key wrap for communication with an remote authentication server. These are provided in the form of AES or Triple-DES keys (with the exception of communications with an authentication server which are only in the form of AES keys).

TOE Evaluated Configuration

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.

Figure 2: Example TOE deployment



The previous figure includes the following:

- Several examples of TOE Models
  - ASA 5505
  - ASA 5510
  - ASA 5520
  - ASA 5540
  - ASA 5550
  - ASA 5580
- VPN Peer (Operational Environment) or another instance of the TOE ASA appliance
- VPN Peer (Operational Environment) with Cisco VPN Client or AnyConnect Client
- Management Workstation (Operational Environment) with ASDM
- Remote Authentication Server (Operational Environment)

- NTP Server (Operational Environment)
- Peer CA (Operational Environment)
- Syslog server (Operational Environment)

Excluded Functionality

The following functionality is excluded from the evaluation:

Excluded Feature	Rationale
Non-FIPS 140-2 mode of operation on the ASA, Cisco AnyConnect Client, or Cisco VPN Client	FIPS 140-2 mode of operation ensures that secure cryptographic algorithms are used for secure operations. Including other modes of operation are unnecessary.
The TTL decrement feature is not to be enabled in the evaluated configuration	While non-interferring, this feature was not tested during the evaluation and therefore is excluded from the evaluated configuration.
SNMP is excluded from the evaluated configuration	While non-interferring, this feature was not tested during the evaluation and therefore is excluded from the evaluated configuration.
Secure Policy Manager is excluded from the evaluated configuration	This legacy software is no longer supported.
Filtering of non-IP traffic provided by the EtherType option when configuring information flow policies is excluded from the evaluated configuration	This feature was not tested during the evaluation and therefore is excluded from the evaluated configuration.
IPS functionality	The additional hardware required to provide IPS functionality was not included in the scope of this evaluation. Therefore, IPS functionality could not be included in the evalution.

Configuration Considerations

The following configuration consideration must be made in the evaluated configuration:

- The TOE must run in Routed Single Context mode only when configured to perform VPN transmissions.
- SSH authentication must use remote AAA server configured for single use authentication.

Conformance Claims

Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 2, dated: September 2007.

The TOE and ST are EAL4 Augmented with ALC_FLR.2 Part 3 conformant.

The TOE and ST are CC Part 2 extended.

Protection Profile Conformance

This ST claims compliance to the following Common Criteria validated Protection Profile:
U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments, Version 1.1, July 25, 2007.

Protection Profile Refinements

The names of all of the Objectives on the Environment were changed from O.XXXXX to OE.XXXXX in this ST.

Protection Profile Additions

The following threats were added to the TOE:

- T.UNTRUSTPATH
- T.UNAUTHPEER
- T.VLAN

The following polices were added to the TOE:

- P.INTEGRITY

The following objectives were added to the TOE:

- O.TRUSTEDPATH
- O.INTEGRITY
- O.KEYCONF
- O.PEERAUTH
- O.VLAN

The following objectives were added to the IT environment:

- OE.NTP
- OE.SYSLOG

The following requirements were added to the set of SFRs on the TOE:

- FCS_CKM.1 (two iterations)
- FCS_CKM.4
- FCS_COP.1 (two more iterations and augmented the existing iteration to cover other uses of AES aside from remote administration also added references to Triple-DES in the SFRs)
- FDP_IFC.1(3)
- FDP_IFC.1(4)
- FDP_IFF.1(3)
- FDP_IFF.1(4)
- FIA_UAU.1
- FMT_MSA.1 (four more iterations)
- FMT_MSA.2
- FMT_MSA.3 (another iteration)
- FMT_SMF.1

- FPT_ITT.1
- FTP_ITC.1
- FCS_COP_(EXT).1
- FCS_IKE_(EXT).1

The following objectives were augmented from the PP:

- O.SELFPRO

The following requirements were augmented from the PP:

- FIA_UAU.5
- FMT_MSA.3
- FMT_SMR.1

Protection Profile Conformance Claim Rationale

TOE Appropriateness

The ASA TOE provides all of the Firewall functionality at a level of security commensurate with that identified in the U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments, Version 1.1, July 25, 2007.

TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target are identical to those from the Protection Profile for which conformance is claimed, with the additions noted above. All concepts covered in the Protection Profile's Security Problem Definitions are included in the Security Target.

Statement of Security Objectives Consistency

The Security Objectives included in the Security Target are identical to those specified in the Protection Profile for which conformance is claimed, with the additions noted above. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

Statement of Security Requirements Consistency

The Security Functional Requirements (SFRs) included in the Security Target are identical to those SFRs specified in the Protection Profile for which conformance is claimed, with the additions noted above. All concepts covered in the Protection Profile's Statement of Security Requirements are included in the Security Target. Additionally, the Security Assurance Requirements included in the Security Target exceed the Security Assurance Requirements included in the Protection Profile.

The objective and requirements that were augmented are included in the table below with a rationale for how they still meet the intent of the PP.

Table 4 Augmented Components

Augmented Component	Augmentation	Rationale
O.SELFPRO	Added "or data" at the end.	The claims requested by the PP are met and exceeded with the addition of "or data" at the end

		of the objective.
FIA_UAU.5	Added bullets for certificate-based and reusable password mechanisms for VPN users.	The PP contained no concept of VPN users, which are not privileged. These users have similar authentication requirements as are required for authorized administrators. This still meets the intent of the PP.
FMT_MSA.3	Added the VPN SFP to the set of security policies with restrictive values.	The PP contains two SFPs, that are both referenced in this SFR. Adding another SFP to the ST and this SFR still meets the intent of the PP.
FMT_SMR.1	Added the VPN user role to the SFR.	The PP contained no concept of VPN users, which are not privileged. Adding a non-privileged role does not violate the intent of the PP.

Security Problem Definition

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- 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 operational 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 5 TOE Assumptions

Assumption Name	Assumption Definition
A.PHYSEC	The TOE is physically secure.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.GENPUR	There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOREMO	Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.

Threats

The following table lists the threats addressed by the TOE and the operational environment. The assumed level of expertise of the attacker for all the threats identified below is enhanced-basic.

Table 6 Threats

Threat Name	Threat Definition
T.NOAUTH	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.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related

	information that is sent between a remotely located authorized administrator and the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.
T. LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
T.TUSAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.
T.UNAUTHPEER	An unauthorized IT entity may attempt to establish a security association with the TOE and violate TOE security policies.
T.UNTRUSTPATH	A malicious user or process may intercept traffic and cause TSF data to be inappropriately accessed (viewed, modified, or deleted) during transfer with a peer.
T.VLAN	An attacker may force a packet destined for one VLAN to cross into another VLAN for which it is not authorized compromising the confidentiality and integrity of information.

Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following table, Organizational Security Policies, identifies the organizational security policies

Table 7 Organizational Security Policies

Policy Name	Policy Definition
P.CRYPTO	AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-2 (level 1).
P.INTEGRITY	The TOE shall support the IETF *Internet Protocol Security Encapsulating Security Payload* (IPSEC ESP) as specified in RFC 2406. Sensitive information transmitted to a VPN peer shall apply integrity mechanisms as specified in *Use of HMAC-SHA-1 within ESP and AH* (RFC 2404).

Security Objectives

This Chapter identifies the security objectives of the TOE and the operational environment. The security objectives identify the responsibilities of the TOE and the TOE's operational 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 operational environment are designated as OE.objective with objective specifying a unique name.

Security Objectives for the TOE

The following table, Security Objectives for the TOE, 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 8 Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network. The TOE must also protect the confidentiality of its dialogue with VPN peers.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions **or data**.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.SECFUN	The TOE must provide functionality that enables an authorized

	administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
O.EAL	The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.
O.TRUSTEDPATH	The TOE will provide a means to ensure users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.
O.INTEGRITY	The TOE must be able to protect the integrity of data transmitted to a peer TOE via encryption and provide IPSec authentication for such data. Upon receipt of data from a peer TOE, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.
O.KEYCONF	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.PEERAUTH	The TOE will authenticate each peer TOE that attempts to establish a security association with the TOE.
O.VLAN	The TOE must provide a means for the logical separation of Virtual LANs to ensure that packets flows are restricted to their authorized Virtual LANs ensuring VLAN separation is achieved.

Security Objectives for the Environment

The assumptions identified previously are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. The following table, Security Objectives for the Environment, identifies the security objectives for the environment.

Table 9 Security Objectives for the Environment

Environment Security Obj.	Operational Environment Security Objective Definition
OE.PHYSEC	The TOE is physically secure.
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.PUBLIC	The TOE does not host public data.

OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
OE.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
OE.NTP	The IT environment may be configured with an NTP server that is able to provide reliable time to the TOE. The communications must be protected using MD5 hashing with up to a 32 character key.
OE.SYSLOG	The IT environment must supply a syslog server capable of receiving SSL-protected TCP syslog information.

Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived verbatim from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, dated: September 2007 and all National Information Assurance Partnership (NIAP) and international interpretations.

Conventions

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:

- Refinement made by PP author: Indicated with **bold** text and strikethroughs, if necessary;
- Refinement made by ST author: Indicated with ***bold italicized*** text and strikethroughs, if necessary;
- Selection: Indicated with underlined text;
- Selection made by ST author: Indicated with *underlined italicized* text;
- Assignment: text in brackets ([ ]);
- Assignment made by ST author: Indicated with *italicized* text in brackets;

- Assignment within a Selection: Indicated with underlined text in brackets;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

Explicitly stated SFRs are identified by having a label '(EXT)' 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 the following table are described in more detail in the following subsections.

Table 10 Security Functional Requirements

SFR Component ID	Component Name
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1(1)	Cryptographic operation – Remote administration and Other Encryption
FCS_COP.1(2)	Cryptographic operation – Hashed Message Authentication Code Generation
FCS_COP.1(3)	Cryptographic operation – SCEP signing
FDP_IFC.1(1)	Subset information flow control
FDP_IFC.1(2)	Subset information flow control
FDP_IFC.1(3)	Subset information flow control
FDP_IFC.1(4)	Subset information flow control
FDP_IFF.1(1)	Simple security attributes
FDP_IFF.1(2)	Simple security attributes
FDP_IFF.1(3)	Simple security attributes
FDP_IFF.1(4)	Simple security attributes
FDP_RIP.1	Subset residual information protection
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms

FIA_UID.2	User identification before any action
FIA_AFL.1	Authentication failure handling
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
FMT_MSA.1(2)	Management of security attributes
FMT_MSA.1(3)	Management of security attributes
FMT_MSA.1(4)	Management of security attributes
FMT_MSA.1(5)	Management of security attributes
FMT_MSA.1(6)	Management of security attributes
FMT_MSA.1(7)	Management of security attributes
FMT_MSA.1(8)	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3(1)	Static attribute initialization
FMT_MSA.3(2)	Static attribute initialization
FMT_MTD.1(1)	Management of TSF data
FMT_MTD.1(2)	Management of TSF data
FMT_MTD.2	Management of limits on TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1	Reliable time stamps
FTP_ITC.1	Inter-TSF trusted channel
Extended Component ID	Component Name
FCS_COP_(EXT).1	Random Number Generation
FCS_IKE_(EXT).1	Internet Key Exchange

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) [the events listed in Table ~~*5.2*~~ ***11***].

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, 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, [information specified in column three of Table 5.2 11].

Table 11 Auditable Events

Functional Component	Auditable Event	Additional Audit Record Content
FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator** role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.5	Any use of the authentication mechanism.	The user identities provided to the TOE
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the authorized administrator of the users capability to authenticate**.	The identity of the offending user and the authorized administrator
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject. Application-specific attributes leading to a denial of flow.
FDP_IFF.1(3)	Errors during IPSec processing, errors during SSL processing	The presumed addresses of the source and destination subject.
FCS_COP.1	Success and failure, and the type of cryptographic operation	The identity of the external IT entity attempting to perform the cryptographic operation
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation

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.

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data based on:

a) [user identity;

b) presumed subject address;

c) ranges of dates;

d) ranges of times;

e) ranges of addresses].

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the authorized administrator and [shall limit the number of audit records lost] if the audit trail is full.

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 [1024, 2048 bits] that meet the following: [PKCS #1 Version 2.1 and ANSI X9.31].

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: [*NIST SP 800-57 "Recommendation for Key Management" Section 6.1*].

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite with zeroes] that meets the following: [*zeroization requirements within FIPS PUB 140-2*].

FCS_COP.1(1) Cryptographic operation – Remote Administration and other Encryption

FCS_COP.1.1(1) The TSF shall perform [encryption of remote authorized administrator sessions, bulk encryption and decryption for SSL VPN, encryption/decryption for IKE and IPSec, and key wrap for remote AAA server communication] in accordance with a specified cryptographic algorithm: [AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67) ***and Triple-DES as specified in FIPS 186-3*** and cryptographic key sizes [that are at least 128 binary digits in length ***(for AES) or are 168 binary digits in length (for Triple-DES)***] that meet the following: [FIPS PUB 140-2 (Level 1)].

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*] and cryptographic key sizes [*160 bit*] that meet the following: [*FIPS 180-1*]

FCS_COP.1(3) Cryptographic operation – SCEP Signing

FCS_COP.1.1(3) The TSF shall perform [digital signing and signature verification for IKE] in accordance with a specified cryptographic algorithm [SHA-1 with RSA Encryption] and cryptographic key sizes [1024 bits] that meet the following: [PKCS#1, ANSI X9.31].

User Data Protection (FDP)

FDP_IFC.1(1) Subset information flow control

FDP_IFC.1.1(1) The TSF shall enforce the [UNAUTHENTICATED SFP] on:

a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;

b) information: traffic sent through the TOE from one subject to another;

c) operation: pass information].

FDP_IFC.1(2) Subset information flow control

FDP_IFC.1.1(2) The TSF shall enforce the [AUTHENTICATED SFP] on:

a) [subjects: a human user or external IT entity that sends and receives FTP and Telnet information through the TOE to one another, only after the human user initiating the information flow has authenticated at the TOE per FIA_UAU.5,

b) information: FTP and Telnet traffic sent through the TOE from one subject to another;

c) operation: initiate service and pass information].

FDP_IFC.1(3) Subset information flow control

FDP_IFC.1.1(3) ***When the TOE is operating in routed single context mode,*** the TSF shall enforce the [VPN SFP] on:

a) [subjects:

- source subject: TOE interface on which information is received;
- destination subject: TOE interface to which information is destined.;

b) information: traffic sent through the TOE from one subject to another;

c) operations:

- encrypt, decrypt, or ignore and pass information].

FDP_IFC.1(4) Subset information flow control

FDP_IFC.1.1(4) The TSF shall enforce the [VLAN SFP] **based** on:

a) [subjects: physical network interfaces;

b) information: Ethernet frame;

c) operations: permit or deny layer two communication.]

FDP_IFF.1(1) Simple security attributes

FDP_IFF.1.1(1) The TSF shall enforce the [UNAUTHENTICATED SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- presumed address;
- none;

b) information security attributes:

- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface or context on which traffic arrives and departs;
- service;
- composition of packets for those protocols listed in Annex A;
- none].

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

a) [Subjects on an internal 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 internal network address;
- the presumed address of the destination subject, in the information, translates to an address on the other connected network or context;
- and the packets for those protocols listed in Annex A conform to their protocol specifications.

b) 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;
- the presumed address of the destination subject, in the information, translates to an address on the other connected network or context;

- and the packets for those protocols listed in Annex A conform to their protocol specifications.]

FDP_IFF.1.3(1) The TSF shall enforce the [none].

FDP_IFF.1.4(1) The TSF shall provide the following [none].

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:

a) [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;

b) 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;

c) 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;

d) 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;

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) For application protocols supported by the TOE (e.g., DNS, HTTP, SMTP, and POP3 and others specified in Annex A), the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC). This shall be accomplished through protocol filtering proxies that are designed for that purpose.

FDP_IFF.1(2) Simple security attributes

FDP_IFF.1.1(2) The TSF shall enforce the [AUTHENTICATED SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- presumed address;
- none;

b) information security attributes:

- user identity;
- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface or context on which traffic arrives and departs;

- service (i.e., FTP and Telnet);
- security-relevant service command;

  composition of packets for those protocols listed in Annex A; and
- *none*].

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

a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:
   - the human user initiating the information flow authenticates according to FIA_UAU.5;
   - 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;
   - he presumed address of the source subject, in the information, translates to an internal network address;
   - the presumed address of the destination subject, in the information, translates to an address on the other connected network or context;
   - and the packets for those protocols listed in Annex A conform to their protocol specifications.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
   - the human user initiating the information flow authenticates according to FIA_UAU.5;
   - 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 the other connected network or context;
   - and the packets for those protocols listed in Annex A conform to their protocol specifications.]

FDP_IFF.1.3(2) The TSF shall enforce the [none].

FDP_IFF.1.4(2) The TSF shall provide the following [none].

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:

a) [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;

b) 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;

c) 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;

d) 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;

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) The TOE shall reject Telnet or FTP command requests that do not conform to generally accepted published protocol definitions (e.g., RFCs). This must be accomplished through protocol filtering proxies designed for that purpose.

FDP_IFF.1(3) Simple security attributes

FDP_IFF.1.1(3) The TSF shall enforce the [*VPN SFP*] based on the following types of subject and information security attributes ***when the TOE is operating in routed single context mode***:

a) [subject security attributes:

- presumed address;

b) information security attributes:

- user identity;
- presumed address of source subject;
- presumed address of destination subject
- transport layer protocol].

FDP_IFF.1.2(3) The TSF shall permit an information flow between a ***source subject and a destination subject*** via a controlled operation if the following rules hold ***when the TOE is operating in routed single context mode***:

- [the user identity is part of the VPN users group;
- the information security attributes match the attributes in a VPN policy rule (contained in the VPN ruleset defined by the Security Administrator) according to the following algorithm [access control policies are followed first, then the VPN flow decision is made]; and

- the selected information flow policy rule specifies that the information flow is to be permitted, and what specific operation from FDP_IFC.1(3) is to be applied to that information flow].

FDP_IFF.1.3(3) The TSF shall enforce the [*following additional rules*] ***when the TOE is operating in routed single context mode***:

- [incoming IPSec or TLS-encapsulated traffic shall be decrypted per FCS_COP.1(1), based on VPN security attributes defined in a VPN policy rule established by the authorised administrator for the security association;
- outgoing traffic shall be encrypted per FCS_COP.1.(1) using IKE/IPSec or TLS, based on VPN security attributes defined in a VPN policy rule established by the authorised administrator for the security association and tunnelled to the VPN peer corresponding to the destination address;
- all traffic that does not match a VPN policy rule shall be ignored and passed.]

FDP_IFF.1.4(3) The TSF shall provide the following [none].

FDP_IFF.1.5(3) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6(3) The TSF shall explicitly deny an information flow based on the following rules ***when the TOE is operating in routed single context mode***:

a) [The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;

b) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;

c) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier;

d) The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject].

FDP_IFF.1(4) Simple security attributes

FDP_IFF.1.1(4) The TSF shall enforce the [*VLAN SFP*] based on the following types of subject and information security attributes:

a) [subject security attributes:

- receiving/transmitting VLAN interface;

b) information security attributes:

- VLAN ID in Header].

FDP_IFF.1.2(4) The TSF shall permit an information flow between a ***source subject and a destination subject*** via a controlled operation if the following rules hold:

- [if the receiving VLAN interface is configured to be in the same VLAN as the transmitting VLAN interface].

FDP_IFF.1.3(4) The TSF shall enforce the [information flow so that only packets contain a matching VLAN ID in the header will be forwarded to the appropriate VLAN interfaces].

FDP_IFF.1.4(4) The TSF shall provide the following [modification of VLAN ID after information flow has been permitted via FDP_IFF.1(1), FDP_IFF.1(2), or FDP_IFF.1(3)].

FDP_IFF.1.5(4) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6(4) The TSF shall explicitly deny an information flow based on the following rules:

[packets associated with a receiving VLAN interface will not be forwarded out a transmitting VLAN interface not configured to be in the same VLAN].

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to [all objects].

Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [a non-zero number determined by the authorized administrator] of unsuccessful authentication attempts occur related to [authorized TOE administrator access or authorized TOE IT entity access].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending user from successfully authenticating until an authorized administrator takes some action to make authentication possible for the user in question].

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) [identity;

b) association of a human user with the authorized administrator role;

c) password or other authentication credential].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [*establishment of ASDM (HTTPS) or SSH session or initiation of VPN sessions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [password and single-use authentication mechanisms] to support user authentication.

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

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

b) single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity;

c) single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user;

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

e) 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

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

FIA_UID.2 User identification before any action

FIA_UID.2.1 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, disable the functions:

a) [operation of the TOE;

b) multiple use authentication functions described in FIA_UAU.5] to [an authorized administrator].

FMT_MOF.1(2) Management of security functions behavior

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

a) [audit trail management;

b) backup and restore for TSF data, information flow rules, and audit trail data; and

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

FMT_MSA.1(1) Management of security attributes

FMT_MSA.1.1(1) The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(1)] to [the authorized administrator].

FMT_MSA.1(2) Management of security attributes

FMT_MSA.1.1(2) The TSF shall enforce the [AUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(2)] to [the authorized administrator].

FMT_MSA.1(3) Management of security attributes

FMT_MSA.1.1(3) The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to delete and [create] the security attributes [information flow rules described in FDP_IFF.1(1)] to [the authorized administrator].

FMT_MSA.1(4) Management of security attributes

FMT_MSA.1.1(4) The TSF shall enforce the [AUTHENTICATED_SFP] to restrict the ability to delete and [create] the security attributes [information flow rules described in FDP_IFF.1(2)] to [the authorized administrator].

FMT_MSA.1(5) Management of security attributes

FMT_MSA.1.1(5) The TSF shall enforce the [*VPN SFP*] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(3)] to [the authorized administrator].

FMT_MSA.1(6) Management of security attributes

FMT_MSA.1.1(6) The TSF shall enforce the [*VPN SFP*] to restrict the ability to delete and [create] the security attributes [vpn rules described in FDP_IFF.1(3)] to [the authorized administrator].

FMT_MSA.1(7) Management of security attributes

FMT_MSA.1.1(5) The TSF shall enforce the [*VLAN SFP*] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(4)] to [the authorized administrator].

FMT_MSA.1(8) Management of security attributes

FMT_MSA.1.1(6) The TSF shall enforce the [*VLAN SFP*] to restrict the ability to delete and [create] the security attributes [vpn rules described in FDP_IFF.1(4)] to [the authorized administrator].

FMT_MSA.2 Secure Security Attributes

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

FMT_MSA.3(1) Static attribute initialization

FMT_MSA.3.1(1) The TSF shall enforce the [UNAUTHENTICATED_SFP and AUTHENTICATED_SFP *and VPN SFP*] to provide restrictive default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) 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_MSA.3(2) Static attribute initialization

FMT_MSA.3.1(2) The TSF shall enforce the [*VLAN SFP*] to provide restrictive default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2(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 query, modify, delete, [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

FMT_MTD.1(2) Management of TSF data

FMT_MTD.1.1(2) The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1.1] to [the authorized administrator].

FMT_MTD.2 Management of limits on TSF data

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [the number of authentication failures] to [the authorized administrator].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [actions specified in FIA_AFL.1.2].

FMT_SMF.1 Specification of Management Functions

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

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

b) Enable or disable the multiple use authentication functions described in FIA_UAU.5;

c) Enable, disable, determine and modify the behavior of the audit trail management;

d) Enable, disable, determine and modify the behavior of the functionality to backup and restore TSF data, information flow rules, and audit trail data;

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

f) Delete attributes from a rule, modify attributes in a rule, add attributes to a rule for all security attributes in FDP_IFF.1(1), (2), and (3);

g) Delete and create attributes/ rules defined in FDP_IFF.1(1), (2), and (3);

h) Query, modify, delete, and assign the user attributes defined in FIA_ATD.1.1;

i) Set the time and date used to form the timestamps in FPT_STM.1.1;

j) Specify the limits for the number of authentication failures.]

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the role [authorized administrator *and VPN user*].

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

Protection of the TSF (FPT)

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between separate parts 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.

Trusted Path/ Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

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

FTP_ITC.1.2 The TSF shall permit *the TSF, another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [OCSP communication with other CAs; TCP syslog transfer to an external syslog server].

Extended Components Definition

This Security Target contains eight Security Functional Requirements that are not drawn from existing CC part 2 Security Function Requirements.

The identification structure of each Security Functional Requirement is modeled after the Security Functional Requirements included in CC part 2. The identification structure includes the following:

A. Class – The extended SFRs included in this ST are part of the FCS class of requirements.

B. Family – The extended SFRs included in this ST are part of several SFR families

C. Component – The extended SFRs are at one component levels: 1.

FCS_COP_(EXT).1 Random Number Generation

FCS_COP_(EXT).1.1 The TSF shall perform all Random Number Generation used by the cryptographic functionality of the TSF using a FIPS-approved Random Number Generator implemented in a FIPS-approved crypto module running in a FIPS-approved mode.

FCS_IKE_(EXT).1 Internet Key Exchange

FCS_IKE_(EXT).1.1 The TSF shall provide cryptographic key establishment techniques in accordance with RFC 2409 as follows(s):

- Phase 1, the establishment of a secure authenticated channel between the TOE and another remote VPN endpoint, shall be performed using one of the following, as configured by the security administrator:
  - Main Mode
  - Aggressive Mode
  - New Group mode shall include one of the following private groups 1 768-bit, 2 1024 bit, 5 1536 bit MOD P,
  - [No other mode].
- Phase 2, negotiation of security services for IPsec, shall be done using Quick Mode, using SHA-1 as the pseudo-random function.

Quick Mode shall generate key material that provides perfect forward secrecy.

FCS_IKE_(EXT).1.2 The TSF shall require the nonce, and the x of g^xy] be randomly generated using FIPS-approved random number generator when computation is being performed.

FCS_IKE_(EXT).1.3 When performing authentication using pre-shared keys, the key shall be generated using the FIPS approved random number generator specified in FCS_COP**_(EXT).1**.

FCS_IKE_(EXT).1.4 The TSF shall compute the value of SKEYID (as defined in RFC 2409), using SHA-1 as the pseudo-random function. The TSF shall be capable of authentication using the methods for

- Signatures: SKEYID = sha(Ni_b | Nr_b, g^xy)
- Pre-shared keys: SKEYID = sha(pre-shared-key, Ni_b | Nr_b)
- [Authentication using Public key encryption, computing SKEYID as follows: SKEYID = sha(sha(Ni_b | Nr_b), CKY-I | Nr_b]

FCS_IKE_(EXT).1.5 The TSF shall compute authenticated keying material as follows:

- SKEYID_d = sha(SKEYID, g^xy | CKY-I | CKY-R | 0)
- SKEYID_a = sha(SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)
- SKEYID_e = sha(SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)
- [none]

FCS_IKE_(EXT).1.6 To authenticate the Phase 1 exchange, the TSF shall generate HASH_I if it is the initiator, or HASH_R if it is the responder as follows:

HASH_I = sha(SKEYID, g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDii_b)

HASH_R = sha(SKEYID, g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDir_b)

FCS_IKE_(EXT).1.7 The TSF shall be capable of authenticating IKE Phase 1 using the following methods as defined in RFC 2409, as configured by the security administrator:

a) Authentication with digital signatures: The TSF shall use [*RSA, "no other digital signature algorithms"*]

b) when an RSA signature is applied to HASH I or HASH R it must be first PKCS#1 encoded. The TSF shall check the HASH_I and HASH_R values sent against a computed value to detect any changes made to the proposed transform negotiated in phase one. If changes are detected the session shall be terminated and an alarm shall be generated.

c) [*X.509 certificates Version 3, [no other versions]*] X.509 V3 implementations, if implemented, shall be capable of checking for validity of the certificate path, and at option of SA, check for certificate revocation.

d) Authentication with a pre-shared key: The TSF shall allow authentication using a pre-shared key.

FCS_IKE_(EXT).1.8 The TSF shall compute the hash values for Quick Mode in the following way:

HASH(1) = sha(SKEYID_a, M-ID | SA | Ni [| KE] [| IDci | IDcr)]

HASH(2) = sha(SKEYID_a, M-ID | Ni_b |SA| Nr [| KE] [| IDci | IDcr)]

HASH(3) = sha(SKEYID_a, 0 | M-ID | Ni_b | Nr_b)

FCS_IKE_(EXT).1.9 The TSF shall compute new keying material during Quick Mode as follows:

[when using perfect forward secrecy

KEYMAT = sha(SKEYID_d, g(qm)^xy | protocol | SPI | Ni_b | Nr_b),

When perfect forward secrecy is not used

KEYMAT = sha(SKEYID_d | protocol | SPI | Ni_b | Nr_b)]

Extended Requirements Rationale

FCS_COP_(EXT).1:

This SFR format was taken from PD-0105 where it is defined as requirement of FCS_IKE_(EXT).1.

FCS_IKE_(EXT).1:

This SFR format was taken from PD-0105 where IKE is defined as an acceptable instance of single-use authentication.

TOE SFR Dependencies

This section of the Security Target demonstrates that the identified TOE and IT Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. The following table lists the TOE Security Functional Components and the Security Functional Components each are 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.

Table 12 Security Functional Requirements

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_SAR.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	Met by FAU_SAR.1
FAU_STG.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_STG.4	FAU_STG.1	Met by FAU_STG.1
FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Met by FCS_COP.1(2), (3), (4), and (5) Met by FCS_CKM.4
FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Met by FCS_COP.1(2), (3), (4), and (5) Met by FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or	Met by FCS_CKM.1

SFR	Dependency	Rationale
	FCS_CKM.1	
FCS_COP.1(1)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Functional component FCS_COP.1 depends on the following functional components: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction and FMT_MSA.2 Secure Security Attributes. Cryptographic modules must be FIPS PUB 140-2 compliant. If the cryptographic module is indeed compliant with this FIPS PUB, then the dependencies of key generation, key destruction and secure key values will have been satisfied in becoming FIPS PUB 140-2 compliant. For more information, refer to section 4.7 of FIPS PUB 140-2. Met by FCS_CKM.1 and FCS_CKM.4 and FMT_MSA.2
FCS_COP.1(2)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Met by FCS_CKM.1(1) and (2) Met by FCS_CKM.4
FCS_COP.1(3)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Met by FCS_CKM.1(1) and (2) Met by FCS_CKM.4
FDP_IFC.1(1)	FDP_IFF.1	Met by FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1	Met by FDP_IFF.1(2)
FDP_IFC.1(3)	FDP_IFF.1	Met by FDP_IFF.1(3)
FDP_IFC.1(4)	FDP_IFF.1	Met by FDP_IFF.1(4)
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(1) Met by FMT_MSA.3(1)
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(2) Met by FMT_MSA.3(1)
FDP_IFF.1(3)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(3) Met by FMT_MSA.3(1)
FDP_IFF.1(4)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(4) Met by FMT_MSA.3(2)
FDP_RIP.1	No dependencies	N/A
FIA_ATD.1	No dependencies	N/A
FIA_UID.2	No dependencies	N/A
FIA_AFL.1	FIA_UAU.1	Met by FIA_UAU.1

SFR	Dependency	Rationale
FIA_UAU.5	No dependencies	N/A
FMT_MOF.1(1)	FMT_SMR.1 FMT_SMF.1	Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MOF.1(2)	FMT_SMR.1 FMT_SMF.1	Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1(1) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1(2) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(3)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1(1) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(4)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1(2) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(5)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1(3) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(6)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1(3) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(7)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1(4) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(8)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1(4) Met by FMT_SMR.1 Met by FMT_SMF.1

SFR	Dependency	Rationale
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	Met by FDP_IFC.1(3) Met by FMT_MSA.1 Met by FMT_SMR.1
FMT_MSA.3(1)	FMT_MSA.1 FMT_SMR.1	Met by FMT_MSA.1 Met by FMT_SMR.1
FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1	Met by FMT_MSA.1 Met by FMT_SMR.1
FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	Met by FMT_SMF.1 Met by FMT_SMR.1
FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	Met by FMT_SMF.1 Met by FMT_SMR.1
FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	Met by FMT_MTD.1 Met by FMT_SMR.1
FMT_SMR.1	FIA_UID.1	Met by FIA_UID.2
FPT_ITT.1	No dependencies	N/A
FPT_STM.1	No dependencies	N/A
FTP_ITC.1	No dependencies	N/A
FCS_COP_(EXT).1	No dependencies	N/A
FCS_IKE_(EXT).1	FCS_COP_(EXT).1	Met by FCS_COP_(EXT).1

TOE Security Assurance Requirements

The TOE assurance requirements for this ST are EAL4 Augmented with ALC_FLR.2 derived from Common Criteria Version 3.1, Revision 2. The Security Target Claims conformance to EAL4 Augmented with ALC_FLR.2. The assurance requirements are summarized in the table below.

Table 13 SAR Requirements

Assurance Class	Components	Components Description
Development	ADV_ARC.1	Architectural Design with domain separation and non-bypassability
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle Support	ALC_CMC.4	Production support, acceptance procedures

Assurance Class	Components	Components Description
		and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC _LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
	ALC_FLR.2	Flaw Reporting Procedures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: security enforcing modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

Security Assurance Requirements Rationale

This Security Target claims conformance to EAL4 Augmented with ALC_FLR.2. This target was chosen to ensure that the TOE has a moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks. Augmentation was chosen to address having flaw remediation procedures and correcting security flaws as they are reported.

The level of security assurance exceeds that which was claimed in the PPs, basic robustness. This level of robustness was chosen for an international applicability. The chosen assurance level is consistent with the postulated threat environment. Specifically, the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low, and the product will have undergone a search for obvious flaws. This is supported by the inclusion of the AVA_VAN.3 requirement.

Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

Table 14 Assurance Measures

Component	How the requirement will be met
ADV_ARC.1	The architecture of the TOE that is used to protect the TSF documented by Cisco in their development evidence.
ADV_FSP.4	The externally visible interfaces of the TOE used by the users of the TOE along with the description of the security functions and a correspondence between the interfaces and the security functions from the ST are documented by Cisco in their development evidence. The development evidence also contains a tracing to the SFRs

Component	How the requirement will be met
	described in this ST.
ADV_IMP.1	Cisco provides access to the TSF implementation to the evaluation lab.
ADV_TDS.3	The design of the TOE will be described in the development evidence. This evidence will also contain a tracing to the TSFI defined in the FSP.
AGD_OPE.1	The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.
AGD_PRE.1	Cisco documents the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.4	Cisco performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE and the implementation representation of the TOE.
ALC_CMS.4	Cisco uniquely identifies configuration items and each release of the TOE has a unique reference. The Configuration Management documentation contains a configuration item list.
ALC_DEL.1	Cisco documents the delivery procedure for the TOE to include the procedure on how to download certain components of the TOE from the Cisco website and how certain components of the TOE are physically delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components.
ALC_DVS.1	Cisco implements security controls over the development environment. Cisco meets these requirements by documenting the security controls.
ALC_FLR.2	Cisco documents the flaw remediation and reporting procedures so that security flaw reports from TOE users can be appropriately acted upon, and TOE users can understand how to submit security flaw reports to the developer.
ALC_LCD.1	Cisco documents the TOE development life-cycle to meet these requirements.
ALC_TAT.1	Cisco uses well-defined development tools for creating the TOE.
ATE_COV.2	Cisco demonstrates the interfaces tested during functional testing using a coverage analysis.
ATE_DPT.2	Cisco demonstrates the TSF subsystems tested during functional testing using a depth analysis.
ATE_FUN.1	Cisco functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of

Component	How the requirement will be met
	the test conducted against the functions specified in the ST.
ATE_IND.2	Cisco will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_VAN.3	Cisco will provide the TOE for testing.

TOE Summary Specification

TOE Security Functional Requirement Measures

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 15 TOE SFRs Measures

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td>FAU_GEN.1</td><td>Shutdown and start-up of the audit functions are logged by events for reloading the ASA, and the events when the ASA comes back up. When audit is enabled, it is on whenever the TOE is on. Also, if logging is ever disabled, it is displayed in the ASDM Real-Time Log Viewer as a syslog disconnection and then a reconnection once it is re-established followed by an event that shows that the "logging enable" command was executed. See the table within this cell for other required events and rationale.
ASA generates events in the following format, with fields for date and time, type of event (the ASA-x-xxxxxx identifier code), subject identities, and outcome of the event:
Jul 21 2008 20:39:21: %ASA-3-713194: Group = 192.168.22.1, IP = 192.168.22.1, Sending IKE Delete With Reason message: Disconnected by Administrator.
<table>
<tr><th>Auditable Event</th><th>Rationale</th></tr>
<tr><td>Modifications to the group of users that are part of the authorized administrator role.</td><td>All changes to the configuration are logged when the logging level is set to at least the 'notifications' level. These changes would fall into the category of configuration changes. The identity of the administrator taking the action and the user being affected (assigned to the authorized administrator role) are both included within the event.</td></tr>
<tr><td>All use of the user identification mechanism.</td><td>Events will be generated for attempted identification/ authentication, and the username attempting to authenticate will be recorded in the event.</td></tr>
<tr><td>Any use of the authentication mechanism.</td><td>Events will be generated for attempted identification/ authentication, and the username attempting to authenticate will be recorded in the event.</td></tr>
<tr><td>The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized</td><td>Failed attempts for authentication will be logged, and when the threshold is reached, it will also be logged. All changes to the configuration are logged when the logging level is set to at least the 'notifications' level.</td></tr>
</table>
</td></tr>
</table>

	administrator of the user's capability to authenticate.	Changes to restore a locked account would fall into the category of configuration changes.
	All decisions on requests for information flow.	In order for events to be logged for information flow requests, the 'log' keyword may need to be in each line of an access control list. The presumed addresses of the source and destination subjects are included in the event.
	Success and failure, and the type of cryptographic operation	Attempts for VPN connections are logged (whether successful or failed). Requests for encrypted session negotiation are logged (whether successful or failed). The identity of the user performing the cryptographic operation is included in the event.
	Changes to the time.	Changes to the time are logged.
	Use of the functions listed in this requirement pertaining to audit.	All changes to the configuration are logged when the logging level is set to at least the 'notifications' level. These changes would fall into the category of configuration changes.
FAU_SAR.1	The ASA is configured to restrict the ability to enter privileged configuration mode to level 15 users (the authorized administrator) once aaa authorizations has been enabled. Privileged configuration (EXEC) mode is where the commands are available to view audit records. They are not available outside of this mode from the CLI. From ASDM, the authorized administrator can also view all audit trail data via the 'Home' screen, the 'Log Buffer', or the 'Real-Time Log Viewer'. Audit records can be viewed by the authorized administrator via the CLI using the 'show logging' command. All audit records (whether viewed locally on the ASA or via ASDM) are stored on the ASA in an internal syslog buffer.	
FAU_SAR.3	The ASA stores the events in order by date. Events are added to the bottom of the buffer display as they are generated, and ASDM displays these new events at the top. The ASDM allows for searches and filtering of the events based on keywords. These audit records can be viewed either locally or remotely (SSH) via the CLI on the ASA or through a viewer in ASDM. The viewer in ASDM allows for filtering of events or searches by keyword and for sorting of events by the header fields in the event viewer: • Severity • Date • Time • Syslog ID • Source ID (User Identity) • Source (Presumed subject address) • Destination ID • Destination (address/ Presumed subject address) Ranges of dates, times can be done through searching for multiple dates and times manually. Ranges of addresses can be done through searching for partial address strings ("192.168.1" to find all addresses from 192.168.1.0/24 subnet). The local audit records on the CLI can be searched using "include" functionality ('show	

	logging | include *x*') and keywords. Sorting of events cannot be done through the CLI.
FAU_STG.1	Audit records can be viewed by the authorized administrator via the CLI using the 'show logging' command. Audit records are stored on the ASA in an internal syslog buffer. This buffer can only be deleted by the authorized administrator using the 'clear logging buffer' command, which can be executed from the CLI or through the ASDM command line executer. The buffer cannot be altered.
FAU_STG.4	As the ASA's internal syslog buffer fills up, it will begin to overwrite the oldest events first. In order to minimize the number of events that will be lost, events can be exported from the server to an external syslog server using TCP syslog connections. In the event that the external server cannot be reached by the ASA new traffic sessions through the ASA will be stopped, and an alert event will be logged to alert the administrator. New VPN sessions will also be denied. The ASA will continue to attempt to connect to the external server five times, and once a connection is re-established new connections will resume. Existing connections will have already been logged and are therefore unaffected during the pause in new flows. The number of events that will be lost is equal to the number of events that it takes the administrator to note the issue, copy events off the system, and clear the logs.
FCS_CKM.1(1) and (2) FCS_CKM.4 FCS_COP.1(1) through (3) FCS_COP_(EXT).1	The ASA has been (will be) FIPS 140-2 certified for use of AES with 128, 192, and 256 bit keys. AES is used in CBC mode and three key Triple-DES with 168 bit keys. The FIPS certification is at FIPS 140-2 Level 2. The certificate number is 1436, and will be filled in before the end of the evaluation. The VPN clients have been verified to be FIPS compliant for versions Cisco VPN Client 5.0.06.0600 and AnyConnect 2.5. The FIPS RNG that is used is the ANSI X9.31 In the TOE crypto is used to establish TLS, HTTPS, and SSH sessions, for IPSec traffic and authentication keys, for IKE authentication and encryption keys, and key wrap for communication with an remote authentication server.
FDP_IFC.1(1) and FDP_IFF.1(1)	The TOE supports the ability to set up rules between interfaces of the ASA for unauthenticated traffic. These rules control whether a packet is transferred from one interface to another based on: 1. presumed address of source 2. presumed address of destination 3. transport layer protocol 4. Service used 5. Network interface on which the connection request occurs Packets will be dropped unless a specific rule has been set up to allow the packet to pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied. These rules are entered in the form of access lists at the CLI (via 'access list' and 'access group' commands) or via ASDM on the 'Configuration > Firewall > Access Rules' screen. Above and beyond access list checks, the ASA also confirms that for the protocols referenced in Annex A that the packets conform to the protocol specifications. The means that if malformed DNS packets are detected that conform to an access list, that they will still be dropped.
FDP_IFC.1 (2) and FDP_IFF.1(2)	The TOE supports the ability to set up rules between interfaces of the ASA for traffic requiring authentication. These rules control whether a packet is transferred from one interface to another based on:

	1. User identity 2. presumed address of source 3. presumed address of destination 4. transport layer protocol 5. Service used 6. Security-relevant service command 7. Network interface on which the connection request occurs Packets will be dropped unless a specific rule has been set up to allow the packet to pass(where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied. Telnet and FTP traffic can be forced to authenticate. These rules are entered in the form of access lists at the CLI (via 'access list' and 'access group' commands) or via ASDM on the 'Configuration > Firewall > Access Rules' screen. Above and beyond access list checks, the ASA also confirms that for the protocols referenced in Annex A that the packets conform to the protocol specifications. The means that if telnet or ftp packets are detected that conform to an access list but are not among the accepted commands specified in the proxy, that they will still be dropped.
FDP_IFC.1(3) and FDP_IFF.1(3)	The TOE facilitates IPSec VPN communication with IPSec enabled IT devices. The TOE compares plaintext traffic received from IPSec VPN or destined to IPsec VPN to the configured information flow policies. If the information flow meets a configured information flow policy that allows the traffic, then traffic originated from a VPN tunnel or destined to a VPN tunnel is permitted. If the information flow meets a configured policy that denies traffic, such traffic is not permitted. The TOE supports the ability to set up VPN rules for the interfaces of the ASA. These rules determine whether or not a packet is sent via an encrypted tunnel to or from the interface based on: 1. User identity 2. Presumed address of source 3. Presumed address of destination VPN tunnels will not be established unless a specific policy allowing them has been set up. Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied. These policies are created in the form of crypto policies at the CLI (via 'crypto map' commands) or via ASDM on the 'Configuration > Remote Access VPN' and 'Configuration > Site-to-Site VPN' pages. The TOE will take the following actions based on the VPN policy: • pass packets without modifying; • send IPSEC encrypted and authenticated packets to a VPN peer using ESP in tunnel mode as defined in RFC 2406; • send TLS encrypted and authenticated packets to a VPN peer over an HTTPS tunnel; • decrypt, verify authentication and pass received packets from a VPN peer in tunnel mode using ESP; • decrypt, verify authentication and pass received packets from a VPN peer in tunnel mode using TLS handshake; Note: the TOE does not support IPv6 IPSec VPNs. The TOE only supports IPSec VPN via

	IPv4.
FDP_IFC.1(4) and FDP_IFF.1(4)	The ASA 5505 comes preconfigured with two VLANs: VLAN1 and VLAN2. By default, Ethernet switch port 0/0 is allocated to VLAN2. All other switch ports are allocated by default to VLAN1. Up to 20 active VLANs are supported on the ASA 5505. Because there are only 8 physical ports, the additional VLANs are useful for assigning to trunk ports, which aggregate multiple VLANs on a single physical port. The ASA 5510, 5520, 5540, 5550, and 5580 do not come preconfigured with any VLANs, however their physical ports can be divided into sub-interfaces using an option on the 'interface' command. Physical ports on the same VLAN communicate with each other using hardware switching. VLANs communicate with each other using routes and bridges. For example, when a switch port on VLAN1 is communicating with a switch port on VLAN2, the adaptive security appliance applies configured security policies to the traffic and routes or bridges the traffic between the two VLANs. To impose strict access control and provide protection of sensitive devices, one can apply security policies to VLANs that restrict communications between VLANs. One can also apply security policies to individual ports. For example, one can allocate each physical port to a separate VLAN, such as Outside, DMZ 1, DMZ 2, Engineering, Sales, Customer Service, Finance, and HR.
FDP_RIP.1	Within the ASA operating 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 TOE accounts for all packets traversing the firewall in relation to the associated information stream. Therefore, no residual information relating to other packets will be reused on that stream.
FIA_AFL.1	For authentication using the internal user authentication database, the ASA enforces lockout settings set using the 'aaa local authentication attempts max-fail number' command (or set through ASDM on 'Configuration > Device Management > Users/AAA > AAA Server Groups' page). The number of failures to be detected and trigger the lockout can be between 1 and 16. NOTE: VPN peers are not locked out by automated mechanisms. The IKEv1 protocol provides a pre-shared key method of an ISAKMP SA establishment, and when this method is used any IKE peer which possesses a pre-shared secret key is considered legitimate due to the anonymous nature of the IKEv1 DH key exchange procedure. Thus, policy based VPN peer lockout can only be achieved by manual methods (e.g. a pre-shared key removal or modification).
FIA_ATD.1	The ASA supports definition of administrators by individual user IDs, and these IDs are associated with a specific privilege level. The highest privilege level being 15, which is the authorized administrator. This associates human users, through their respective IDs, with the authorized administrator role. Through the CLI the 'username' and 'password' commands is used to maintain, create, and delete users and maintain their attributes. Through ASDM this is done on the 'Configuration > Device Management > Users/AAA > User Accounts' page. Certificates can also be used for SSL VPN authentication with the TOE. These certificates are used through integration with TACACS+, RADIUS, and other remote authentication servers.
FIA_UAU.5.1	The ASA supports integration with TACACS+, RADIUS, and other remote authentication servers that support single-use authentication passwords, certificates, and IKE. These servers can be used for single-use authentication of administrators (both local serial console and remote), IT entities, and traffic. Through the CLI the 'aaa server' is used to establish connections with external authentication

	servers, while the ability to utilize the internal user authentication database for authentication is configured with the 'aaa authentication local' command. Through ASDM this is done on the 'Configuration > Device Management > Users/AAA > AAA Server Groups' and 'Configuration > Device Management > Users/AAA > AAA Access > Authentication' pages respectively. **NOTE:** The TSF polls the NTP server. Hence, FIA_UAU.5 does not apply because the TSF accesses the NTP server rather than the other way around.
FIA_UID.2 and FIA_UAU.1	In the evaluated configuration, once the aaa authentication settings are in-place, there is no CLI access without identification and authentication. By default, ASDM uses the internal users authentication database for identification and authentication. No access is allowed without encountering one of these authentication prompts. The only actions that can be taken prior to authentication is establishment of an HTTPS or SSH session on behalf of the administrator, or initiation of VPN sessions on behalf of a VPN user. These sessions are negotiated at the request of the administrator and VPN user, and the cryptographic settings are negotiated between the various clients/ browsers and the TOE without the input of the administrator or VPN user.
FMT_MOF.1(1)	The ASA is configured to restrict the ability to enter privileged configuration mode to level 15 users (the authorized administrator). Privileged configuration (EXEC) mode is where the commands are available to modify all settings, including authentication settings. They are not available outside of this mode. The ASDM uses the same privileges that the user would have at the CLI to determine access to administrative functions in the ASDM GUI.
FMT_MOF.1(2)	The ASA is configured to restrict the ability to enter privileged configuration mode to level 15 users (the authorized administrator) once aaa authorizations has been enabled. Privileged configuration (EXEC) mode is where the commands are available to modify all settings, including authentication settings. They are not available outside of this mode. The following commands are used for each item in the SFR: enable: 'logging enable'; disable: 'no logging enable'; determine/ modify: 'show config', 'logging', 'clear logging buffer'; review: 'show logging' archive audit trail data: 'logging savelog', 'copy' (or tftp copy); backing up the config: 'write memory' (copy running-config start-config) and then 'tftp copy'; restoring a saved config: 'tftp copy', then 'copy flash:[x config] running-config', then 'write memory' 'ssh' (use 'interface' keyword to specify/ limit interfaces); '(no) snmp server'; '(no) telnet'; 'http server enable'; 'http' (with the 'interface' keyword) The ASDM uses the same privileges that the user would have at the CLI to determine access to administrative functions in the ASDM GUI.
FMT_MSA.1(1) FMT_MSA.1(2) FMT_MSA.1(3) FMT_MSA.1(4) FMT_MSA.1(5) FMT_MSA.1(6) FMT_MSA.1(7) and FMT_MSA.1(8)	The ASA access policies are configured to protect the ASA itself and to restrict the ability to enter privileged configuration mode to level 15 users (the authorized administrator). See the rationale for FMT_SMF.1, below, for the commands used to meet the functionality. The ASDM uses the same privileges that the user would have at the CLI to determine access to administrative functions in the ASDM GUI. This means that the same user can authenticate to either the CLI or ASDM and result in the same set of privileges.
FMT_MSA.2	By default, when the TOE is running in FIPS mode, the defined encryption functions will not operate with key sizes or algorithms that are not FIPS compliant.

FMT_MSA.3(1) and FMT_MSA.3(2)	By default, all interfaces on the ASA are disabled, and when they are enabled they must have a security level assigned to them (between 0 and 100). The default is that traffic is only allowed to flow from higher security levels to lower levels and to deny all traffic from lower security levels to higher.
FMT_MTD.1(1) FMT_MTD.1(2) and FMT_MTD.2	The ASA is configured to restrict the ability to enter privileged configuration mode to level 15 users (the authorized administrator) once aaa authorizations has been enabled. Privileged configuration (EXEC) mode is where the commands are available to modify user attributes. They are not available outside of this mode. See the rationale for FMT_SMF.1, below, for the commands used to meet the functionality. The ASDM uses the same privileges that the user would have at the CLI to determine access to administrative functions in the ASDM GUI.
FMT_SMF.1	The ASA is configured to restrict the ability to enter privileged configuration mode to level 15 users (the authorized administrator) once aaa authorizations has been enabled. Privileged configuration (EXEC) mode is where the commands are available to modify user attributes (‘username’ and ‘password’ commands), operation of the TOE (‘reload’), authentication functions (‘aaa’ commands'), audit trail management (‘logging’ commands), backup and restore of TSF data (‘copy’ commands), communication with authorized external IT entities (‘ssh’ and ‘access list’ commands), information flow rules (‘access list’ commands), modify the timestamp (‘clock’ commands), and specify limits for authentication failures (‘aaa local authentication lockout’) . These commands are not available outside of this mode. Communications with external IT entities, include the host machine for ASDM. This is configured through the use of ‘https’ commands that enable communication with the host and limit the IP addresses from which communication is accepted. The ASDM uses the same privileges that the user would have at the CLI to determine access to administrative functions in the ASDM GUI. All administrative configuration is done through the ‘Configuration’ page.
FMT_SMR.1	The ASA supports multiple levels of administrators, the highest of which is a privilege 15. In this evaluation privilege 15 would be the equivalent of the authorized administrator. Multiple level 15 administrators with individual usernames can be created. Through the CLI the ‘username’ command is used to maintain, create, and delete users. Through ASDM this is done on the ‘Configuration > Device Management > Users/AAA > User Accounts’ page. Users within the single local database are distinguished based on their privilege level (0-15) and service tag. The following applies when authentication and "exec" authorization are enabled: In order to be authorized for "enabled" access, i.e, access to the privileged prompt, the user must have the ADMINISTRATIVE access service tag. Note that users in the local DB are automatically given ADMINISTRATIVE access if the service-type attribute is not otherwise configured. 'aaa authentication ssh console LOCAL' sets the ASA to authenticate SSH users against the local database. 'aaa authorization exec' requires authorization of users before they can get to the exec console.
FPT_ITT.1	The communication between the ASA and the ASDM is protected via HTTPS session. This protects the data from disclosure by encryption within the SSL protocol, and by checksums that verify that data has not been modified. The communication between the ASA and the VPN client for delivery of certificates is protected via PKCS12 encrypted containers. This protects the certificate from disclosure and

	modification during delivery.
FPT_STM.1	The ASA provides a source of date and time information for the firewall, 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 firewall. The clock function is reliant on the system clock provided by the underlying hardware. This functionality can be set at the CLI using the 'clock' commands or in ASDM through the 'Configuration > Device Setup > System Time' page. The TOE can optionally be set to receive time from an NTP server.
FTP_ITC.1	The ASA includes a Local CA feature. For revocation, the ASA performs revocation checking using OCSP or CRLs when validating the client certificate (if enabled). The ASA also protects communications with a remote syslog server via SSL.
FCS_IKE_(EXT).1	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. 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, and • The agreement of secure bulk data encryption Triple-DES (168-bit) /AES (128, 192 or 256 bit) keys for use with ESP. 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. The TOE generates secure RSA public/private keys (1024 and 2048 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. For two peers to succeed in establishing an SA, they must have at least one compatible (match) crypto map. 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 internal user authentication database mechanism or an external authentication server for Xauth user authentication.

TOE Bypass and interference/logical tampering Protection Measures

The ASA TOE consists of a hardware and software solution. The ASA hardware platform protects all operations in the TOE appliance scope from interference and tampering by untrusted subjects. All TSP enforcement functions must be invoked and succeed prior to functions within the TSC proceeding.

The TOE has been designed so that all locally maintained TSF data can only be manipulated via the secured management interface, a CLI, a GUI (ASDM) interface. There are no undocumented interfaces for managing the product.

All sub-components included in the TOE hardware rely on the main ASA chassis for power, memory management, and access control. In order to access any portion of the TOE, the Identification & Authentication mechanisms of the ASA must be invoked and succeed.

No processes outside of the ASA are allowed direct access to any TOE memory. The TOE only accepts traffic through legitimate TOE interfaces. None of these interfaces provide any access to internal TOE resources.

The ASA provides a secure domain for each context to operate within. Each context has its own resources that other contexts within the same ASA platform are not able to affect.

Finally, the ASA enforces information flow control and VPN policies and applies network traffic security on its interfaces before traffic passes into or out of the TOE. The TOE controls every ingress and egress traffic flow. Policies are applied to each traffic flow. Traffic flows characterized as unauthorized are discarded and not permitted to circumvent the TOE.

There are no unmediated traffic flows into or out of the TOE. The information flow policies identified in the SFRs are applied to all traffic received and sent by the ASA. Each communication is mediated by the TOE. There is no opportunity for unaccounted traffic flows to flow into or out of the TOE.

The Cisco ASDM, VPN Client, and AnyConnect Client, as software implementations, are dependent upon the operational environment. These software components run on the operating systems identified in Table 2, above. These components use crypto libraries from the host operating systems to do IPSec

and SSL/TLS connections to the ASA. On Linux and Mac platforms the clients use the libcurl libraries, which in turn rely on OpenSSL. On Windows platforms (including Windows Mobile) the clients use the WinInet libraries, which perform crypto using the building in Microsoft Cryptographic API (MSCAPI).

This design, combined with the fact that only an administrative user with the appropriate role may access the TOE security functions, provides a distinct protected domain for the TOE that is logically protected from interference and is not bypassable.

Rationale

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined within this Security Target. The table below illustrates the mapping from Security Objectives to Threats and Policies.

Rationale for the TOE Security Objectives

Table 16 Summary of Mappings Between Threats and IT Security Objectives

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T.LOWEXP	T.UNAUTHPEER	T.UNTRUSTPATH	T.VLAN	P.CRYPTO	P.INTEGRITY
O.IDAUTH	X															
O.SINUSE		X	X													
O.MEDIAT				X	X	X										
O.SECSTA	X								X							
O.ENCRYP	X						X								X	
O.SELPRO	X								X	X						
O.AUDREC								X								
O.ACCOUN								X								
O.SECFUN	X		X							X						
O.LIMEXT	X															
O.EAL											X					
O.TRUSTEDPATH													X			
O.INGEGRITY																X
O.KEYCONF													X			
O.PEERAUTH												X				
O.VLAN														X		

O.IDAUTH This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.

O.SINUSE This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.

O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

O.SECSTA This security objective ensures that no information is compromised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

O.ENCRYP This security objective is necessary to counter the threats and policy: T.NOAUTH, T.PROCOM and P.CRYPTO by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely.

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO, T.AUDFUL and T.NOAUTH because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

O.LIMEXT This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.

O.EAL This security objective is necessary to counter the threat: T.LOWEXP because it requires that the TOE is resistant to penetration attacks performed by an attacker possessing minimal attack potential.

O.TRUSTEDPATH This security objective is necessary to counter the threat: T.UNTRUSTPATH because it ensures that a trusted communication path exists between the TOE and VPN peers.

O.INTEGRITY This security objective is necessary to counter the policy: P.INTEGRITY by ensuring that all IPSEC encrypted data received from a VPN peer is properly decrypted and authentication verified.

O.KEYCONF This security objective is necessary to counter the threat T.UNTRUSTPATH because it ensures that cryptographic keys cannot be captured and used to decrypt packet flows.

O.PEERAUTH This security objective is necessary to counter the threat T.UNAUTHPEER because it ensures that peers must be authenticated to the TOE using strong mechanisms.

O.VLAN This security objective is necessary to counter the threat T.VLAN because it ensures that the TOE will be correctly configured in accordance with a security policy which will ensure VLAN separation.

Rationale for the Security Objectives for the Environment

Table 17 Summary of Mappings Between Threats and Security Objectives for the Environment

	T.USAGE	T.AUDACC
OE.GUIDAN	X	X
OE.ADMTRA	X	X
OE.NTP	X	
OE.SYSLOG	X	

Since the rest of the security objectives for the environment are, in part, a re- statement of the security assumptions, those security objectives trace to all aspects of the assumptions.

OE.PHYSEC The TOE is physically secure.

OE.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

OE.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

O.PUBLIC The TOE does not host public data.

OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

OE.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

OE.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

OE.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

OE.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

OE.GUIDAN This non-IT security objective is necessary to counter the threat: T.TUSAGE and T.AUDACC because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

OE.ADMTRA This non-IT security objective is necessary to counter the threat: T.TUSAGE and T.AUDACC because it ensures that authorized administrators receive the proper training.

OE.NTP This security objective is used to counter the threat: T.USAGE because it ensures that if an NTP server is used that an external party cannot modify the time communications with the server.

OE.SYSLOG This security objective is used to counter the threat: T.USAGE because it ensures that syslog communications between the TOE and the external syslog server cannot be modified.

Rationale for SFRs-SARs/TOE Objectives

This section provides rationale for the Security Functional Requirements/Security Assurance Requirements demonstrating that the Security Functional Requirements/Security Assurance Requirements are suitable to address the security objectives. The table below illustrates the mapping from SFRs to Security Objectives.

Table 18 Summary of Mappings Between IT Security Objectives and SFRs

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT	O.EAL	O.TRUSTEDPATH	O.INGEGRITY	O.KEYCONF	O.PEERAUTH	O.VLAN
FAU_GEN.1							X	X								
FAU_SAR.1							X									
FAU_SAR.3							X									
FAU_STG.1				X		X			X							
FAU_STG.4				X		X			X							
FCS_CKM.1(1)														X		
FCS_CKM.1(2)														X		
FCS_CKM.4														X		
FCS_COP.1(1)					X						X					
FCS_COP.1(2)												X				
FCS_COP.1(3)												X				
FDP_IFC.1(1)			X													
FDP_IFC.1(2)			X													
FDP_IFC.1(3)												X	X			
FDP_IFC.1(4)																X
FDP_IFF.1(1)			X													
FDP_IFF.1(2)			X													
FDP_IFF.1(3)												X	X			
FDP_IFF.1(4)																X
FDP_RIP.1			X													
FIA_ATD.1	X								X							
FIA_UAU.1	X	X														
FIA_UAU.5	X	X														
FIA_UID.2	X							X								
FIA_AFL.1						X										
FMT_MOF.1(1)				X					X	X						
FMT_MOF.1(2)				X					X	X						

FMT_MSA.1(1)			X	X					X							
FMT_MSA.1(2)			X	X					X							
FMT_MSA.1(3)			X	X					X							
FMT_MSA.1(4)			X	X					X							
FMT_MSA.1(5)			X	X					X							
FMT_MSA.1(6)			X	X					X							
FMT_MSA.1(7)			X	X					X							
FMT_MSA.1(8)			X	X					X							
FMT_MSA.2														X		
FMT_MSA.3(1)			X	X												
FMT_MSA.3(2)			X	X												
FMT_MTD.1(1)									X							
FMT_MTD.1(2)									X							
FMT_MTD.2									X							
FMT_SMF.1									X							
FMT_SMR.1									X							
FPT_ITT.1					X											
FPT_STM.1							X									
FTP_ITC.1	X					X										
FCS_COP_(EXT).1					X							X				
FCS_IKE_(EXT).1															X	

FAU_GEN.1 Audit data generation
This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review
This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review
This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage
This component is chosen to ensure that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.

FAU_STG.4 Prevention of audit data loss
This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.

FCS_CKM.1 Cryptographic key generation (1)
This component ensures that keys used for encryption and signatures are generated in accordance to specified algorithms and key sizes. This component traces back to and aids in meeting the following objective: O.KEYCONF.

FCS_CKM.1 Cryptographic key generation (2)
This component ensures that keys used for encryption and signatures are generated in accordance to specified algorithms and key sizes. This component traces back to and aids in meeting the following objective: O.KEYCONF.

FCS_CKM.4 Cryptographic key destruction
This component ensures that keys used for encryption and signatures are generated in accordance to specified algorithms and key sizes. This component traces back to and aids in meeting the following objective: O.KEYCONF.

FCS_COP.1 Cryptographic operation (1)
This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that AES is used to encrypt such traffic. This component ensures the confidentiality of transmissions through strong encryption. This component traces back to and aids in meeting the following objectives: O.ENCRYP and O.EAL.

FCS_COP.1 Cryptographic operation (2) and (3)
This component ensures that a message authentication code is generated and used therefore its authenticity can be established cryptographically. It also supports the protected communication with the CA to check that the digital certificate is trustworthy. This component traces back to and aids in meeting the following objective: O.TRUSTEDPATH.

FDP_IFC.1 Subset information flow control (1)
This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFC.1 Subset information flow control (2)
This component identifies the entities involved in the AUTHENTICATED information flow control SFP (i.e., users of the services FTP or Telnet sending information to servers and vice versa). The users of these services must be authenticated at the TOE. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFC.1 Subset information flow control (3)
This component satisfies this policy by ensuring that all IPSEC encrypted data received from a peer TOE is properly decrypted and authentication verified. This component traces back to and aids in meeting the following objectives: O.TRUSTEDPTH and O.INTEGRITY.

FDP_IFC.1 Subset information flow control (4)
This component satisfies this policy by ensuring that all VLAN traffic sent and received is correctly separated from other VLAN traffic. This component traces back to and aids in meeting the following objective: O.VLAN.

FDP_IFF.1 Simple security attributes (1)
This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes (2)
This component identifies the attributes of the users sending and receiving the information in the AUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes (3)
This component satisfies this policy by ensuring that all IPSEC encrypted data received from a peer TOE is properly decrypted and authentication verified. This component traces back to and aids in meeting the following objectives: O.TRUSTEDPTH and O.INTEGRITY.

FDP_IFF.1 Simple security attributes (4)
This component satisfies this policy by ensuring that all VLAN traffic sent and received is correctly separated from other VLAN traffic. This component traces back to and aids in meeting the following objective: O.VLAN.

FDP_RIP.1 Subset residual information protection
This component ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FIA_AFL.1 Authentication failure handling
This component ensures that human users who are not authorized administrators can not endlessly attempt to authenticate. After some number of failures that the authorized administrator decides, that must not be zero, the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.

FIA_ATD.1 User attribute definition
This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.

FIA_UAU.1 Timing of authentication
This component ensures that before anything occurs on behalf of a user, the user's identity is authenticated to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_UAU.5 Multiple authentication mechanisms
This component was chosen to ensure that multiple authentication mechanism are used appropriately in all attempts to authenticate at the TOE from an internal or external network. A SOF metric for this requirement is defined in section 5.1.1 to ensure that the mechanisms are of adequate probabilistic strength to protect against authentication data compromise. This component traces back to and aids in meeting the following objective: O.SINUSE and O.IDAUTH.

FIA_UID.2 User identification before any action
This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FMT_MOF.1 Management of security functions behavior (1)
This component was to ensure the TSF restricts the ability of the TOE start up and shut down operation and multiple authentication function to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

FMT_MOF.1 Management of security functions behavior (2)
This component was to ensure the TSF restricts the ability to modify the behavior of functions such as audit trail management, back and restore for TSF data, and communication of authorized external IT entities with the TOE to an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

FMT_MSA.1 Management of security attributes (1)
This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to delete, modify, and add within a rule those security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (2)
This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to delete, modify, and add within a rule those specified security attributes that are listed in section FDP_IFF1.1(2). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (3)
This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (4)
This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(2). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (5)
This component ensures the TSF enforces the VPN SFP to restrict the ability to delete, modify, and add within a rule those specified security attributes that are listed in section FDP_IFF1.1(3). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (6)
This component ensures the TSF enforces the VPN SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(3). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (7)
This component ensures the TSF enforces the VLAN SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(4). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (8)
This component ensures the TSF enforces the VLAN SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(4). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.2 Secure Security Attributes
This component ensures that keys used for encryption and signatures are generated in accordance to

specified algorithms and key sizes. This component traces back to and aids in meeting the following objective: O.KEYCONF.

FMT_MSA.3(1) Static attribute initialization
This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECSTA.

FMT_MSA.3(2) Static attribute initialization
This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECSTA.

FMT_MTD.1 Management of TSF data (1)
This component ensures that the TSF restrict abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.1 Management of TSF data (2)
This component ensures that the TSF restrict abilities to set the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.2 Management of limits on TSF data
This component ensures that the TSF restrict the specification of limits of the number of unauthenticated failures to the authorized administrator and specifies the action be taken if limits on the TSF data are reached or exceeded. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_SMF.1 Specification of Management Functions
This component ensures that the TSF restrict the set of management functions to the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_SMR.1 Security roles
Each of the CC class FMT components in this Protection Profile depends on this component. It requires the PP/ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

FPT_ITT.1 Basic internal TSF data transfer protection
This component ensures that the TSF requires protection of the administrative traffic between the ASDM component and the ASA, and the VPN client and the ASA for certificate delivery. This traces back to and aids in meeting the following objective: O.ENCRYP.

FPT_STM.1 Reliable time stamps
FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FTP_ITC.1 Basic internal TSF data transfer protection
This component ensures that the TSF requires protection of the certificate traffic between the ASA and the remote syslog server, and the ASA and other Certificate Authorities. This traces back to and aids in meeting the following objectives: O.IDAUTH and O.SELPRO.

FCS_COP_(EXT).1 Random Number Generation
This component supports all of the encryption functionality on the TOE by providing the randomization.. This component traces back to and aids in meeting the following objectives: O.ENCRYP and O.TRUSTEDPATH.

FCS_IKE_(EXT).1 Internet Key Exchange
The O.PEERAUTH objective is satisfied by this component, which specifies that the TOE must implement the Internet Key Exchange protocol defined in RFC 2409. By implementing this protocol, the TOE will establish a secure, authenticated channel with each peer TOE for purposes of establishing a security association, which includes the establishment of a cryptographic key, algorithm and mode to be used for all communication. It is possible to establish multiple security associations between two peer TOEs, each with its own cryptographic key. Authentication may be via a digital signature or pre-shared key.

Glossary: Acronyms and Abbreviations

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

Table 19 Acronyms or Abbreviations

Acronym or Abbreviation	Definition
CC	Common Criteria
DH	Diffie Hellman (DH) Key Technique used to exchange private encryption keys.
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
IPSec	IP tunneling protocol that manages encryption between multiple hosts using secure communication
PP	Protection Profile
SA	Security Association
SAR	Security Assurance Requirements
SFP	Security Function Policy
SFR	Security Functional Requirements
SSL	Secure Sockets Language
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

Glossary: References and Related Documents

The following documentation was used to prepare this ST:

[FWPP] "U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments," Version 1.1, July 25, 2007.

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2006, version 3.1, Revision 1, CCMB-2006-09-001

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2007, version 3.1, Revision 2, CCMB--2007-09-002

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2007, version 3.1, Revision 2, CCMB-2007-09-003

[CEM] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2007, version 3.1, Revision 2, CCMB-2007-09-004

Annex A: Application Inspection

Advanced application inspection is supported for the following protocols:

For IPv4:

IPv4 Protocol
H.323
DNS
ICMP
FTP
GTP
HTTP
ILS
IPSec-Pass-Thru
MGCP
NetBIOS
PPTP
RSH
RTSP
Skinny
SIP
ESMTP
SNMP
SunRPC
TFTP
XDMCP

For IPv6:

IPv6 Protocol
FTP
HTTP
ICMP
SIP
SMTP
TCP
UDP

Obtaining Documentation, 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