



# **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 evaluated solution is the Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform solutions running ASA 8.4(4.1) with Cisco AnyConnect, or Cisco VPN Client. 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  
September 2012**

**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

© 2012 Cisco Systems, Inc. All rights reserved.  
This document may be freely reproduced and distributed whole and intact including this copyright notice

---

# Table of Contents

Table of Contents	2
List of Tables	4
List of Figures	5
Security Target Introduction	5
ST and TOE Identification	5
TOE Overview	6
TOE Product Type	6
Supported non-TOE Hardware/ Software/ Firmware	7
TOE Description	8
Physical Scope of the TOE	10
Logical Scope of the TOE	11
VPN and/or Firewall Information Flow Control	12
IPSec VPN	12
SSL VPN	13
Single or Multiple Context	14
Routed or Transparent Mode	14
Audit	15
Identification & Authentication	15
Management	16
Cryptography	16
TOE Evaluated Configuration	17
Excluded Functionality	18
Configuration Considerations	18
Conformance Claims	18
Common Criteria Conformance Claim	18
Protection Profile Conformance	18
Protection Profile Refinements	19

---

Protection Profile Additions	19
Protection Profile Conformance Claim Rationale	21
TOE Appropriateness	21
TOE Security Problem Definition Consistency	21
Statement of Security Objectives Consistency	22
Statement of Security Requirements Consistency	22
Security Problem Definition	22
Assumptions	23
Threats	23
Organizational Security Policies	25
Security Objectives	26
Security Objectives for the TOE	26
Security Objectives for the Environment	28
Security Requirements	29
Conventions	29
TOE Security Functional Requirements	30
Security audit (FAU)	32
Cryptographic Support (FCS)	36
User Data Protection (FDP)	37
Identification and Authentication (FIA)	43
Security Management (FMT)	45
Protection of the TSF (FPT)	47
Resource Utilization (FRU)	47
TOE Access (FTA)	48
Trusted Path/ Channels (FTP)	48
Extended Components Definition	49
Security audit (FAU)	49
Cryptographic Support (FCS)	49
Identification and Authentication (FIA)	52
Protection of the TSF (FPT)	53

---

TOE Access (FTA) **Error! Bookmark not defined.**

Extended Requirements Rationale 53

TOE SFR Dependencies 55

TOE Security Assurance Requirements 59

    Security Assurance Requirements Rationale 60

    Assurance Measures 60

TOE Summary Specification 61

    TOE Security Functional Requirement Measures 61

    TOE Bypass and interference/logical tampering Protection Measures 74

Rationale 75

    Rationale for the TOE Security Objectives 75

    Rationale for the Security Objectives for the Environment 78

    Rationale for SFRs-SARs/TOE Objectives 79

Glossary: Acronyms and Abbreviations 90

Glossary: References and Related Documents 92

Annex A: Application Inspection 93

Obtaining Documentation, Support, and Security Guidelines 94

## List of Tables

Table 1	ST and TOE Identification	5
Table 2	TOE Component Identification	7
Table 3	Physical Scope of the TOE	10
Table 4	Augmented Components	22
Table 5	TOE Assumptions	23
Table 6	Threats	23
Table 7	Organizational Security Policies	25
Table 8	Security Objectives for the TOE	26
Table 9	Security Objectives for the Environment	28
Table 10	Security Functional Requirements	30
Table 11	Auditable Events	32
Table 12	Security Functional Requirements	55
Table 13	SAR Requirements	59
Table 14	Assurance Measures	60
Table 15	TOE SFRs Measures	62
Table 16	Summary of Mappings Between Threats and IT Security Objectives	76
Table 17	Summary of Mappings Between Threats and Security Objectives for the Environment	78

Table 18	Summary of Mappings Between IT Security Objectives and SFRs	79
Table 19	Acronyms or Abbreviations	90

## List of Figures

Figure 1: ASA Appliances	9
Figure 2: Example TOE deployment	17

## Security Target Introduction

The Security Target contains the following sections:

- Security Target Introduction 4
- TOE Description 8
- Conformance Claims 18
- Security Problem Definition 22
- Security Objectives 26
- Security Requirements 29
- TOE Summary Specification 61
- Rationale 75

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	September 2012
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform, version 8.4(4.1)
TOE Hardware Models	Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40, 5585-S10, 5585-S20, 5585-S40, and 5585-S60
TOE Software Version	Cisco ASA Release 8.4(4.1), Cisco AnyConnect Release 3.0.08057, Cisco VPN Client Releases 5.0.07.0410 or 5.0.07.0440, Cisco Adaptive Security Device Manager (ASDM) 6.4(9)

ST Evaluation Status	In Evaluation
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 Secure Socket Layer (SSL) encryption to secure connections between remote users and specific, supported internal protected resources. AnyConnect uses the Datagram Transport Layer Security (DTLS) and 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 TOE Component Identification**

Operational Environment Component	Required	Usage/ Purpose Description for TOE performance
VPN Peer	No	<p>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.</p> <p>Note that there are two VPN clients that are considered part of the TOE, and they are not included in this category.</p>
VPN Client Platform	Yes	<p>This includes the platform and OS for both the Cisco AnyConnect Release 3.0.08057 and Cisco VPN Client Release 5.0.07.0410 or 5.0.07.0440.</p> <p>The AnyConnect client operates on any of the following OSs:</p> <ul style="list-style-type: none"> <li>• Windows XP (x86), including Service Pack 1, 2, and 3</li> <li>• Windows Vista (x86 and x64), including Service Pack 1 and 2</li> <li>• Windows 7 (x86 and x64)</li> <li>• Apply Mac OS X 10.5 (Intel only) and 10.6 (PowerPC and Intel) (x86 and x64)</li> <li>• Linux: Red Hat Enterprise Linux 5 Desktop and Ubuntu 9.x and 10.x</li> </ul> <p>The VPN Client operates on any of the following OSs:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows XP (x86 and x64), including Service Pack 1, 2, and 3</li> <li>• Windows Vista platform (x86 and x64) including Service Pack 1 and 2</li> <li>• Windows 7 (x86 and x64)</li> <li>• Apply Mac OS X 10.4 - 10.6 (x86 and x64)</li> </ul>

Operational Environment Component	Required	Usage/ Purpose Description for TOE performance
ASDM Management Platform	Yes	<p>The ASDM 6.4(9) operates from any of the following operating systems:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows XP (x86), including Service Pack 1, 2, and 3</li> <li>• Windows Vista (x86 and x64), including Service Pack 1 and 2</li> <li>• Windows 7 (x86 and x64)</li> <li>• Mac OS X 10.4 - 10.6 (x86 and x64)</li> </ul> <p>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.</p>
Webbrowser	No	<p>The following web browsers are supported for access to the ASDM;</p> <ul style="list-style-type: none"> <li>• Internet Explorer (6 or higher)</li> <li>• Firefox (3 or higher)</li> <li>• Safari (3 or higher)</li> </ul>
Remote Authentication Server	Yes	<p>A RADIUS or TACACS+ server is required for use with the TOE. If these remote AAA servers will be used to authenticate ASA administrators, they should provide password complexity controls and account lockout controls consistent with those provided in Cisco ASA, as defined in FIA_PMG_EXT1 and FIA_AFL.1.</p>
NTP Server	No	<p>The TOE supports communications with an NTP server, with support for NTPv3 recommended.</p>
Peer Certificate Authority (CA)	No	<p>The TOE supports OCSP communication with other CAs.</p>
Syslog Server	Yes	<p>A syslog server with the capability to support SSL-protected TCP syslog communications is required for use with the TOE.</p>

## 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 8.4(4.1). Cisco ASA-5505, ASA-5510, ASA-5520, ASA-5540, ASA-5550, ASA-5580-20, 5580-40, 5585-S10, 5585-S20, 5585-S40, and 5585-S60 each with the following processor and interface configurations:
  - 5505 – 500 MHz AMD Geode LX (GX3) – Eight 10/100 copper Ethernet ports
  - 5510 – 1.6 GHz Intel 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 Intel Celeron – Four 10/100/1000 copper Ethernet ports, one out-of-band management port
  - 5540 – 2.0 GHz Intel Pentium 4 – Four 10/100/1000 copper Ethernet ports, one out-of-band management port
  - 5550 – 3.0 GHz Intel Pentium 4 – Eight Gigabit Ethernet ports, four small form factor-pluggable (SFP) fiber ports, one Fast Ethernet port
  - 5580-20 – Two 2.6GHz AMD Opteron – Two RJ-45 management Gigabit Ethernet 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 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)

- 5585-S10 – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), eight Gigabit Ethernet ports (expandable to sixteen), two 10 Gigabit Ethernet SFP+ fiber ports (expandable to four),
- 5585-S20 – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), eight Gigabit Ethernet ports (expandable to sixteen) and a two 10 Gigabit Ethernet SFP+ fiber ports (expandable to four)
- 5585-S40 – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to twelve) and a four 10 Gigabit Ethernet SFP+ fiber ports (expandable to eight)
- 5585-S60 – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to twelve) and a four 10 Gigabit Ethernet SFP+ fiber ports (expandable to eight)
- VPN clients: The following VPN clients are included with the TOE.
  - Cisco AnyConnect Release 3.0.08057 (including Cisco SSL VPN Clientless software)
  - Cisco VPN Client Release 5.0.07.0410 or 5.0.07.0440
- ASDM software: The ASDM 6.4(9) 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 8.4(4.1), 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 8.4(4.1), 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 8.4(4.1), including a Linux Kernel 2.6

<p>ASA 5540</p> 	<p>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.</p>	<p>ASA release 8.4(4.1), including a Linux Kernel 2.6</p>
<p>ASA 5550</p> 	<p>The Cisco ASA 5550 Adaptive Security Appliance provides high-performance firewall and VPN services via eight Gigabit Ethernet interfaces, four Small Form-Factor Pluggable (SFP) fiber interfaces, and support for up to 250 VLANs.</p>	<p>ASA release 8.4(4.1), including a Linux Kernel 2.6</p>
<p>ASA 5580-20 ASA 5580-40</p> 	<p>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 1024 VLANs.</p>	<p>ASA release 8.4(4.1), including a Linux Kernel 2.6</p>
<p>ASA-5585-S10 ASA-5585-S20 ASA-5585-S40 ASA-5585-S60</p> 	<p>The Cisco ASA 5585 Adaptive Security Appliance provides high-performance firewall and VPN services and 6-16 Gigabit Ethernet interfaces, 2-10 10Gigabit Ethernet interfaces, and support for up to 1024 VLANs.</p>	<p>ASA release 8.4(4.1), including a Linux Kernel 2.6</p>
<p>Cisco AnyConnect (including Cisco SSL VPN Clientless software)</p>	<p>Not applicable</p>	<p>Release 3.0.08057</p>
<p>Cisco VPN Client</p>	<p>Not applicable</p>	<p>5.0.07.0410 or 5.0.07.0440</p>
<p>ASDM 6.4(9)</p>	<p>Not applicable</p>	<p>Release 6.4(9)</p>

## Logical Scope of the TOE

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

- VPN and/or Firewall Information Flow Control
- Audit
- Identification & Authentication
- Management

- 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:

- User identities (source and/or destination)
- Presumed address of source subject
- Presumed address of destination subject
- Service used
- Transport layer protocol
- Security-relevant service command
- 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.

The TOE can be configured to export audit events to an external SYSLOG server. Communication with that server can be protected using SSL and the TOE can determine when communication with the SYSLOG server fails and can be configured to stop forwarded traffic should that occur.

## 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.

The TOE can be configured to display an advisory banner when administrators log in and also to terminate administrator sessions after a configured period of inactivity.

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. ASA administrators can also configure a banner to be displayed to VPN users connecting with AnyConnect or the VPN Client components of the ToE.

---

## 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:

- Enable or disable the operation of the TOE.
- Enable or disable the multiple use authentication functions.
- Enable, disable, determine and modify the behavior of the audit trail management.
- Enable, disable, determine and modify the behavior of the functionality to backup and restore TSF data, information flow rules, and audit trail data.
- Enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE.
- Delete and create attributes/ rules for VPN and information flow.
- Delete attributes from a rule, modify attributes in a rule, add attributes to a rule.
- Query, modify, delete, and assign the user attributes.
- Set the time and date used to form the timestamps.
- 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 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 Cisco VPN Client uses cryptography at two abstraction levels:

- 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.
- 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:

- Session setup: Here cryptography is used as part of the protocol used to set-up HTTPS sessions using TLS.
- 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.

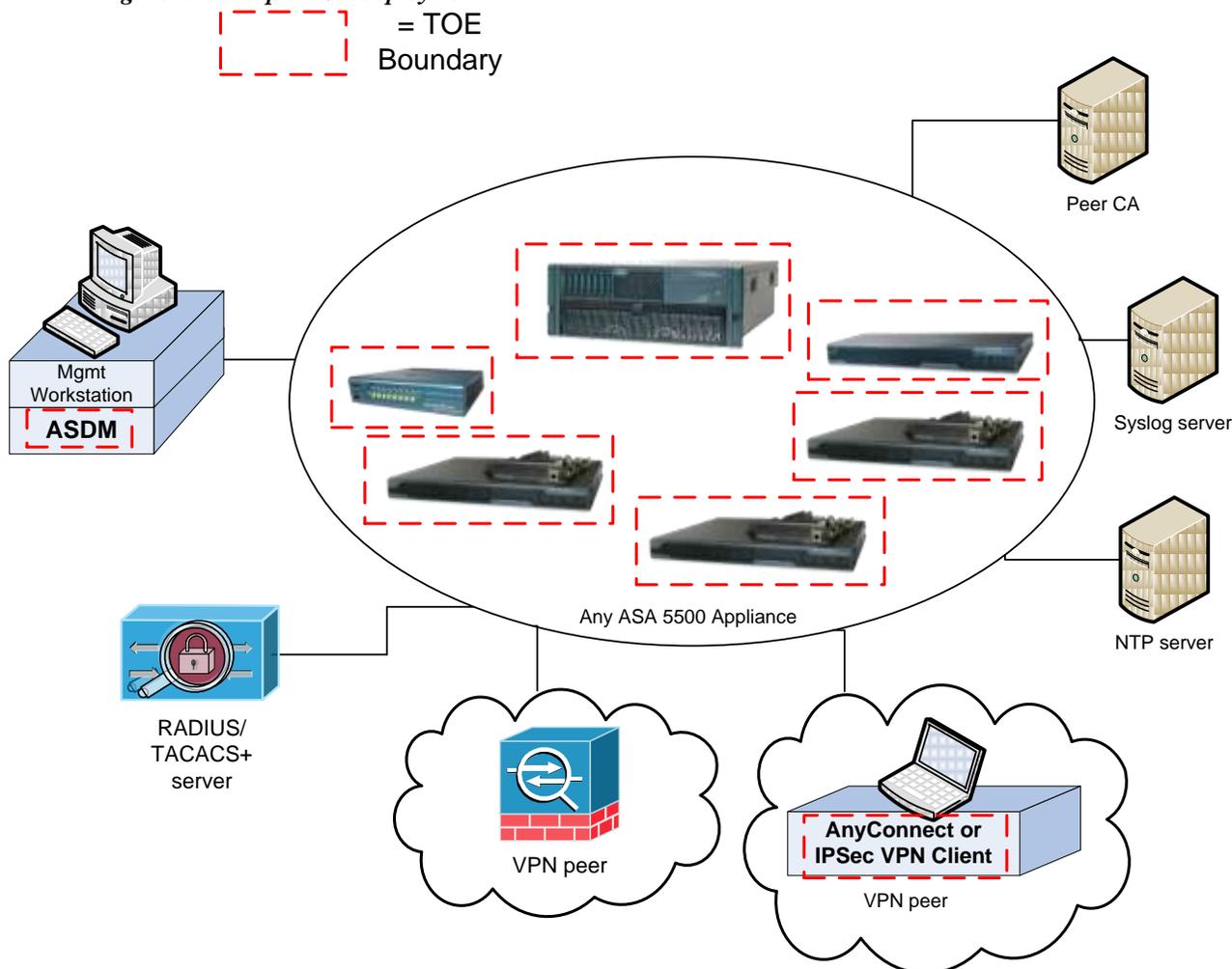
The ASA uses cryptography in the following forms:

- Identity certificates for the ASA itself, and also for use in IPSEC, TLS, and SSH negotiations. This is provided by RSA keys.
- Key agreement for IKE, TLS, and SSH sessions. This is provided by Diffie-Hellman.
- For TLS traffic keys, SSH session keys, IPsec authentication keys, IPsec traffic keys, IKE authentication keys, and IKE encryption keys. These are provided in the form of AES or Triple-DES 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 (e.g., 5505, 5510, 5520, 5540, 5550, 5580-x, and 5585-x)
  - 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:

- The TTL decrement feature is not to be enabled in the evaluated configuration.
- SNMP is excluded from the evaluated configuration
- Secure Policy Manager is excluded from the evaluated configuration
- Filtering of non-IP traffic provided by the EtherType option when configuring information flow policies is excluded from the evaluated configuration

### **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 CC part 3 conformant.

The claimed assurance package is EAL4 augmented with ALC\_FLR.2.

The TOE and ST are CC Part 2 extended.

### **Protection Profile Conformance**

- This ST claims compliance to the following Common Criteria validated Protection Profile (PP):
- U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments, Version 1.1, July 25, 2007 [FWPP]
- This ST has adopted the Security Problem Definition, Security Objectives, and Security Functional Requirements (SFRs) from the following PP to demonstrate support for the evolution of that new PP, but does not claim conformance to accommodate current customer demand for higher assurance (e.g., EAL4) evaluations.

- Security Requirements for Network Devices, Version 1.0, 10 December 2010 [NDPP]

### Protection Profile Refinements

- The names of all of the Objectives on the Environment were changed from O.XXXXXX to OE.XXXXXX in this ST.
- A.PHYSEC was modified to reflect the TOE boundary includes not just the physical Firewall and VPN Gateway appliance, but also the VPN client software that resides on VPN user workstations.
- O.EAL was modified to reflect the increased EAL from the PP (defined for EAL2) and this ST (EAL4) in which the TOE must be resistant to attackers possessing an Enhanced-Basic attack potential as defined within the [CEM].
- T.LOWEXP and OE.LOWEXP were renamed to T.ENHEXP and OE.ENHEXP respectively to reflect the increased EAL from the PP (defined as EAL2) for environments with low/basic attack potential to EAL4 for use in environments with enhanced attack potential.
- FAU\_STG.1 was refined to be specific to protection of audit records while they're stored locally on the TOE in order to avoid any confusion with FAU\_STG\_EXT.1, which is specific to protection of audit records transmitted to a remote audit server.

### Protection Profile Additions

The following threats were added to the TOE:

- T.UNTRUSTPATH
- T.UNAUTHPEER
- T.VLAN
- T.ADMIN\_ERROR
- T.RESOURCE\_EXHAUSTION
- T.TSF\_FAILURE
- T.UNAUTHORIZED\_ACCESS
- T.UNAUTHORIZED\_UPDATE
- T.UNDETECTED\_ACTIONS
- T.USER\_DATA\_REUSE

The following polices were added to the TOE:

- P.INTEGRITY
- P.ACCESS\_BANNER

The following objectives were added to the TOE:

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

- O.VLAN
- O.DISPLAY\_BANNER
- O.PROTECTED\_COMMUNICATIONS
- O.RESIDUAL\_INFORMATION\_CLEARING
- O.RESOURCE\_AVAILABILITY
- O.SESSION\_LOCK
- O.SYSTEM\_MONITORING
- O.TOE\_ADMINISTRATION
- O.TSF\_SELF\_TEST
- O.VERIFIABLE\_UPDATES

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:

- FAU\_GEN.2
- FAU\_STG\_EXT.1
- FAU\_STG\_EXT.3
- FCS\_CKM.1 (three iterations)
- FCS\_CKM.4
- FCS\_COP.1 (four iterations)
- FCS\_HTTPS\_EXT.1
- FCS\_IKE\_EXT.1
- FCS\_RBG\_EXT.1
- FCS\_SSH\_EXT.1
- FCS\_TLS\_EXT.1
- FDP\_IFC.1 (two more iterations)
- FDP\_IFF.1 (two more iterations)
- FIA\_PMG\_EXT.1
- FIA\_UAU.1
- FIA\_UAU.6
- FIA\_UAU.7
- FIA\_UAU\_EXT.5
- FMT\_MSA.1 (four more iterations)

- FMT\_MSA.2
- FMT\_MSA.3 (one more iteration)
- FMT\_MTD.1 (one more iteration)
- FMT\_SMF.1
- FPT\_ITT.1 (two iterations)
- FPT\_PTD\_EXT.1
- FPT\_PTD\_EXT.2
- FPT\_RPL.1
- FPT\_TST\_EXT.1
- FPT\_TUD\_EXT.1
- FRU\_RSA.1
- FTA\_SSL.3
- FTA\_TAB.1
- FTP\_ITC.1 (two iterations)
- FTP\_TRP.1 (two iterations)

The following objectives were augmented from the PP:

- O.SELFPRO

The following requirements were augmented from the PP:

- FAU\_GEN.1
- FDP\_RIP.2
- 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*

<b>Augmented Component</b>	<b>Augmentation</b>	<b>Rationale</b>
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.
FAU_GEN.1	Added additional required audit events.	The claim has been extended to also require additional auditable events related to additional functional claims.
FDP_RIP.2	Upgraded FDP_RIP.1 to FDP_RIP.2	The PP targets only network packets while the TOE ensures residual information is properly handled for all objects.
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 <i>hardware component of the</i> TOE is physically secure.
A. <b>LOWEXPENHEXP</b>	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered <b>low enhanced</b> .
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.

**\*Note:** The assumptions A.GENPUR, and A.PUBLIC and their corresponding objectives for the operational environment OE.GENPUR, and OE.PUBLIC are drawn from the FWPP and relate only to the firewall appliance component of the TOE containing a web server for remote administration from ASDM. These Assumptions and Objectives are irrelevant to the VPN client components of the TOE that are incapable of ‘hosting’ any data.

## 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
-------------	-------------------

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. <del>LOWEXPEN</del> HEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered <del>low</del> -enhanced.
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 VPN security association with the TOE and violate TOE

Threat Name	Threat Definition
	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 remote VPN endpoint (client or gateway).
T.VLAN	An attacker may attempt to force a frame from for one VLAN to cross into another VLAN for which it is not authorized compromising the integrity of the admin-defined traffic flows.
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.RESOURCE_EXHAUSTION	A process or user may deny access to TOE services by exhausting critical resources on the TOE.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF by an attacker or unauthorized user.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender, resulting in unintended disclosure of user data to an attacker.

## 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

Policy Name	Policy Definition
	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 <i>Internet Protocol Security Encapsulating Security Payload</i> (IPSEC ESP) as specified in RFC 2406. Sensitive information transmitted to a VPN peer shall apply integrity mechanisms as specified in <i>Use of HMAC-SHA-1 within ESP and AH</i> (RFC 2404).
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

## 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

TOE Security Obj.	TOE Security Objective Definition
	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 <i>or data</i> .
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 attackers possessing Enhanced-Basic attack potential.
O.TRUSTEDPATH	The TOE will provide a means to ensure VPN 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 remote VPN endpoint (client or gateway) via encryption and provide VPN tunnel authentication for such data. Upon receipt of data from a remote VPN endpoint, 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 VPN endpoint and when kept in short and long-term storage.
O.PEERAUTH	The TOE will authenticate each peer TOE that attempts to establish a VPN security association with the TOE.
O.VLAN	The TOE must provide a means for the logical separation of Virtual LANs (VLANs) that will ensure packet flows are restricted to their authorized VLANs

TOE Security Obj.	TOE Security Objective Definition
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.PROTECTED_COMMUNICATIONS	The TOE will provide properly protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.RESOURCE_AVAILABILITY	The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage).
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.

## 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 <i>hardware component of the</i> TOE is physically secure.
OE. <del>LOWEXPENHEXP</del>	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered <i>enhanced</i> .
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.

Environment Security Obj.	Operational Environment Security Objective Definition
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.
OE.SYSLOG	The IT environment must supply a syslog server capable of receiving SSL-protected TCP syslog information.

**\*Note:** The assumptions A.GENPUR, and A.PUBLIC and their corresponding objectives for the operational environment OE.GENPUR, and OE.PUBLIC are drawn from the FWPP and relate only to the firewall appliance component of the TOE containing a web server for remote administration from ASDM. These Assumptions and Objectives are irrelevant to the VPN client components of the TOE that are incapable of 'hosting' any data.

## 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 3, dated: July 2009 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_GEN.2	User identity association
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(1)	Cryptographic key generation – RSA
FCS_CKM.1(2)	Cryptographic key generation – Diffie-Hellman
FCS_CKM.1(3)	Cryptographic key generation (for asymmetric keys)
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1(1)	Cryptographic operation – Remote administration and Other Encryption
FCS_COP.1(2)	Cryptographic Operation (for keyed-hash message authentication)
FCS_COP.1(3)	Cryptographic Operation (for cryptographic signature)
FCS_COP.1(4)	Cryptographic Operation (for cryptographic hashing)
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.2	Full Residual Information Protection
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition

<b>SFR Component ID</b>	<b>Component Name</b>
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6	Re-authenticating
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.2	User identification before any action
FMT_MOF.1(1)	Management of security functions behavior
FMT_MOF.1(2)	Management of security functions behavior
FMT_MSA.1(1)	Management of security attributes
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_RPL.1	Replay Detection
FPT_STM.1	Reliable time stamps
FRU_RSA.1	Maximum Quotas
FTA_SSL.3	TSF-initiated Termination
FTA_TAB.1	Default TOE Access Banners
FTP_ITC.1(1)	Inter-TSF Trusted Channel (Prevention of Disclosure)
FTP_ITC.1(2)	Inter-TSF Trusted Channel (Detection of Modification)
FTP_TRP.1(1)	Trusted Path

SFR Component ID	Component Name
FTP_TRP.1(2)	Trusted Path
Extended Component ID	Component Name
FAU_STG_EXT.1	External Audit Trail Storage
FAU_STG_EXT.3	Action in case of Loss of Audit Server Connectivity
FCS_HTTPS_EXT.1	Explicit: HTTPS
FCS_IKE_EXT.1	Internet Key Exchange
FCS_IPSEC_EXT.1	Explicit: IPSEC
FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
FCS_SSH_EXT.1	Explicit: SSH
FCS_TLS_EXT.1	Explicit: TLS
FIA_PMG_EXT.1	Password Management
FIA_UAU_EXT.5	Extended: Password-based Authentication Mechanism
FPT_PTD_EXT.1	Management of TSF Data (for reading of authentication data)
FPT_PTD_EXT.2	Management of TSF Data (for reading of all symmetric keys)
FPT_TST_EXT.1	TSF Testing
FPT_TUD_EXT.1	Extended: Trusted Update

## 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:
- Start-up and shutdown of the audit functions;
  - All auditable events for the not specified level of audit; and
  - [the events listed in Table 11].
- FAU\_GEN.1.2 The TSF shall record within each audit record at least the following information:
- Date and time of the event, type of event, subject identity, outcome (success or failure) of the event; and
  - 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 11].

**Table 11 Auditable Events**

Functional Component	Auditable Event	Additional Audit Record Content
FAU_GEN.1	None.	

Functional Component	Auditable Event	Additional Audit Record Content
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FAU_STG_EXT.3	Loss of connectivity.	No additional information.
FCS_CKM.1(3)	Failure on invoking functionality.	No additional information.
FCS_COP.1(1)	Success and failure, and the type of cryptographic operation	The identity of the external IT entity attempting to perform the cryptographic operation
FCS_COP.1(2)	Failure on invoking functionality.	No additional information.
FCS_COP.1(3)	Failure on invoking functionality.	No additional information.
FCS_COP.1(4)	Failure on invoking functionality.	No additional information.
FCS_IPSEC_EXT.1	Failure to establish a IPSEC Session. Establishment/Termination of a IPSEC Session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session. Establishment/Termination of a HTTPS Session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	Failure of the randomization process.	No additional information.
FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS Session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_SSH_EXT.1	Failure to establish an SSH Session. Establishment/Termination of an SSH Session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
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.

Functional Component	Auditable Event	Additional Audit Record Content
FDP_RIP.2	None.	
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent <b>restoration by the authorized administrator of the users capability to authenticate.</b>	The identity of the offending user and the authorized administrator
FIA_PMG_EXT.1	None.	
FIA_UAU.5	Any use of the authentication mechanism.	The user identities provided to the TOE
FIA_UAU_EXT.5	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.6	Attempt to re-authenticate.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE
FMT_MOF.1(1)	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation
FMT_MOF.1(2)	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation
FMT_SMF.1	All administrator actions.	
FMT_SMR.1	Modifications to the group of users that are part of <b>the authorized administrator</b> role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FPT_ITT.1	None.	
FPT_PTD_EXT.1	None.	
FPT_PTD_EXT.2	None.	
FPT_RPL.1	Detected replay attacks.	Origin of the attempt (e.g., IP address).
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation The old and new values for the time.

Functional Component	Auditable Event	Additional Audit Record Content
		Origin of the attempt (e.g., IP address)
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	Indication that TSF self-test was completed.	Any additional information generated by the tests beyond “success” or “failure”. SCHEME needs to be consulted.
FRU_RSA.1	Maximum quota being exceeded.	Resource identifier.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_TAB.1	None.	
FTP_ITC.1(1)	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_ITC.1(2)	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1(1)	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.
FTP_TRP.1(2)	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

**FAU\_GEN.2 User identity association**

FAU\_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

**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.
<b>FAU_SAR.3</b>	<b>Selectable audit review</b>
FAU_SAR.3.1	The TSF shall provide the ability to perform searches and sorting of audit data based on: <ul style="list-style-type: none"> <li>a) [user identity;</li> <li>b) presumed subject address;</li> <li>c) ranges of dates;</li> <li>d) ranges of times;</li> <li>e) ranges of addresses].</li> </ul>
<b>FAU_STG.1</b>	<b>Protected audit trail storage</b>
FAU_STG.1.1	The TSF shall protect the <b>locally</b> stored audit records from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to prevent modifications to the audit records.
<b>FAU_STG.4</b>	<b>Prevention of audit data loss</b>
FAU_STG.4.1	The TSF shall <u>prevent auditable events, except those taken by the authorized administrator</u> 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.1(3) Cryptographic key generation (for asymmetric keys)

FCS\_CKM.1.1(3) The TSF shall generate *asymmetric* cryptographic keys *in accordance with a domain parameter generator and [a random number generator]* that meet the following: [

- *ANSI X9.80 (3 January 2000), “Prime Number Generation, Primality Testing, and Primality Certificates” using random integers with deterministic tests, or constructive generation methods*
- *Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 112 bits using conservative estimates.*
- *For domain parameters used in RSA-based key establishment schemes NIST Special Publication 800-56B “Recommendation for Pair-Wise*

**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 (for data encryption/decryption including remote administration)**

FCS\_COP.1.1(1) The TSF shall perform [encryption of remote authorized administrator sessions, bulk encryption and decryption for SSL VPN, and encryption/decryption for IKE and IPSec] in accordance with a specified cryptographic algorithm: [AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67 and 800-38A) and Triple-DES as specified in FIPS 186-3] and cryptographic key sizes [that are at least 128 or 256 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 (for keyed-hash message authentication)**

FCS\_COP.1.1(2) The TSF shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm [HMAC-SHA-1], and cryptographic key sizes [160 bits], and message digest sizes 160 bits that meet the following: [FIPS Pub 198-1 “The Keyed-Hash Message Authentication Code”, and FIPS PUB 180-3, “Secure Hash Standard.”]

**FCS\_COP.1(3) Cryptographic operation (for cryptographic signature)**

FCS\_COP.1.1(3) The TSF shall perform [cryptographic signature services] in accordance with a [RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 1024, 2048 bits or greater] that meets the following:

[For RSA Digital Signature Algorithm (rDSA): FIPS PUB 186-2, “Digital Signature Standard”]

**FCS\_COP.1(4) Cryptographic operation (for cryptographic hashing)**

FCS\_COP.1.1(4) The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [SHA-1, SHA-2] and ~~cryptographic key~~ message digest sizes [160, 256, 512] bits that meet the following: [FIPS Pub 180-3 “Secure Hash Standard”]

**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;
- a) 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 authorized 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:  
 [frames 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.2 Full residual information protection**

FDP\_RIP.2.1 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].
<b>FIA_ATD.1</b>	<b>User attribute definition</b>
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: <ul style="list-style-type: none"> <li>a) [identity;</li> <li>b) association of a human user with the authorized administrator role;</li> <li>c) password or other authentication credential].</li> </ul>
<b>FIA_UAU.1</b>	<b>Timing of authentication</b>
FIA_UAU.1.1	The TSF shall allow [ <i>establishment of ASDM (HTTPS) or SSH session or initiation of VPN sessions</i> ] 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.
<b>FIA_UAU.5</b>	<b>Multiple authentication mechanisms</b>
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: <ul style="list-style-type: none"> <li>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;</li> <li>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;</li> <li>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;</li> <li>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.</li> <li>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</li> <li>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].</li> </ul>

<b>FIA_UAU.6</b>	<b>Re-authenticating</b> FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions: <i>[when the user changes their password, no other conditions]</i> .
<b>FIA_UAU.7</b>	<b>Protected authentication feedback</b> FIA_UAU.7.1	The TSF shall provide only <i>[obscured feedback]</i> to the user while the authentication is in progress at the local console.
<b>FIA_UID.2</b>	<b>User identification before any action</b> 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 <u>enable, disable</u> 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 <u>enable, disable, determine and modify the behavior</u> 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 <u>delete</u> 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 <u>delete</u> 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].
<b>FMT_MSA.1(6) Management of security attributes</b>	
FMT_MSA.1.1(6)	The TSF shall enforce the [VPN SFP] to restrict the ability to <u>delete</u> and [create] the security attributes [vpn rules described in FDP_IFF.1(3)] to [the authorized administrator].
<b>FMT_MSA.1(7) Management of security attributes</b>	
FMT_MSA.1.1(7)	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].
<b>FMT_MSA.1(8) Management of security attributes</b>	
FMT_MSA.1.1(8)	The TSF shall enforce the [VLAN SFP] to restrict the ability to <u>delete</u> and [create] the security attributes [VLAN rules described in FDP_IFF.1(4)] to [the authorized administrator].
<b>FMT_MSA.2 Secure Security Attributes</b>	
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for [cryptographic security attributes].
<b>FMT_MSA.3(1) Static attribute initialization</b>	
FMT_MSA.3.1(1)	The TSF shall enforce the [UNAUTHENTICATED_SFP and AUTHENTICATED_SFP and VPN SFP] to provide <u>restrictive</u> default values for <b>information flow</b> 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.
<b>FMT_MSA.3(2) Static attribute initialization</b>	
FMT_MSA.3.1(2)	The TSF shall enforce the [VLAN SFP] to provide <u>restrictive</u> default values for <b>information flow</b> 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.
<b>FMT_MTD.1(1) Management of TSF data</b>	
FMT_MTD.1.1(1)	The TSF shall restrict the ability to <u>query, modify, delete,</u> [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].
<b>FMT_MTD.1(2) Management of TSF data</b>	
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].
<b>FMT_MTD.2 Management of limits on TSF data</b>	
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].
<b>FMT_SMF.1 Specification of Management Functions</b>	
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), (3), and (4);
- g) Delete and create attributes/ rules defined in FDP\_IFF.1(1), (2), (3), and (4);
- 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;
- k) Ability to configure the list of TOE services available before an entity is identified and authenticated, as specified in FIA\_UID.2, respectively;
- l) Ability to configure the cryptographic functionality;
- m) Ability to update the TOE, and to verify the updates using the published hash (FCS\_COP.1(4)).]

**FMT\_SMR.1 Security roles**  
 FMT\_SMR.1.1  
 FMT\_SMR.1.2

The TSF shall maintain the role [authorized administrator *and* VPN user].  
 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\_RPL.1 Replay detection**  
 FPT\_RPL.1.1

The TSF shall detect replay for the following entities: [network packets terminated at the TOE].

FPT\_RPL.1.2

The TSF shall perform: [reject the data] when replay is detected.

**FPT\_STM.1 Reliable time stamps**  
 FPT\_STM.1.1

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

**Resource Utilization (FRU)**

**FRU\_RSA.1 Maximum quotas**  
 FRU\_RSA.1.1

The TSF shall enforce maximum quotas of the following resources: [number of interactive administrative sessions], [no other resource] that [authorized administrators] can use [simultaneously].

## TOE Access (FTA)

### FTA\_SSL.3 TSF-initiated termination

FTA\_SSL.3.1 The TSF shall terminate **local and remote** interactive sessions after a [Authorized Administrator-configurable time interval of session inactivity].

### FTA\_TAB.1 Default TOE Access Banners

FTA\_TAB.1.1 Before establishing *an user-administrator* session the TSF shall display *an authorized administrator-specified advisory notice and consent* warning message regarding unauthorized use of the TOE.

## Trusted Path/ Channels (FTP)

### FTP\_ITC.1(1) Inter-TSF trusted channel (prevention of disclosure)

FTP\_ITC.1.1(1) The TSF shall **use** [IPSEC, OCSP, SSL, TLS, and DTLS] to provide a **trusted** communication channel between itself and **authorized IT entities** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure.

FTP\_ITC.1.2(1) The TSF shall permit the TSF, **or the authorized IT entities** to initiate communication via the trusted channel.

FTP\_ITC.1.3(1) The TSF shall initiate communication via the trusted channel for [all authentication functions, [VPN connections, exporting audit records to an external server, and certificate traffic with external CAs]].

### FTP\_ITC.1(2) Inter-TSF trusted channel (detection of modification)

FTP\_ITC.1.1(2) The TSF shall **use** [IPSEC, OCSP, SSL, TLS, and DTLS] **in providing** a **trusted** communication channel between itself and **authorized IT entities** that is logically distinct from other communication channels and provides assured identification of its end points and **detection of the modification of data**.

FTP\_ITC.1.2(2) The TSF shall permit the TSF, **or the authorized IT entities** to initiate communication via the trusted channel.

FTP\_ITC.1.3(2) The TSF shall initiate communication via the trusted channel for [all authentication functions, [VPN connections, exporting audit records to an external server, and certificate traffic with external CAs]].

### FTP\_TRP.1(1) Trusted path (prevention of disclosure)

FTP\_TRP.1.1(1) The TSF shall provide a communication path between itself and *remote administrators* **using** [SSH or TLS/HTTPS] that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure.

FTP\_TRP.1.2(1) The TSF shall permit **remote administrators** to initiate communication via the trusted path.

FTP\_TRP.1.3(1) The TSF shall require the use of the trusted path for [all remote administrative actions].

### FTP\_TRP.1(2) Trusted path (detection of modification)

FTP\_TRP.1.1(2) The TSF shall provide a communication path between itself and *remote administrators* **using** [SSH or TLS/HTTPS] that is logically distinct from other communication paths and provides assured identification of its end points and detection of modification of the communicated data.

FTP_TRP.1.2(2)	The TSF shall permit <b>remote administrators</b> to initiate communication via the trusted path.
FTP_TRP.1.3(2)	The TSF shall require the use of the trusted path for [all remote administrative actions].

## Extended Components Definition

This Security Target contains two 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 identified classes of requirements.
- B. Family – The extended SFRs included in this ST are part of several SFR families
- C. Component – The extended SFRs are not hierarchical to any other components, though they may have identifiers terminating on other than “1”. The dependencies for each extended component are identified in the TOE SFR Dependencies section of this ST below.

### Security audit (FAU)

#### FAU\_STG\_EXT.1 External audit trail storage

FAU\_STG\_EXT.1.1 The TSF shall be able to [transmit the generated audit data to an external IT entity over a trusted channel defined in FTP\_ITC.1].

#### FAU\_STG\_EXT.3 Action in case of loss of audit server connectivity

FAU\_STG\_EXT.3.1 The TSF shall [*block new permit actions*] if the link to the external IT entity collecting the audit data generated by the TOE is not available.

### Cryptographic Support (FCS)

#### FCS\_HTTPS\_EXT.1 HTTPS

FCS\_HTTPS\_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS\_HTTPS\_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS\_TLS\_EXT.1.

#### 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 authorized 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_RBG_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 <ul style="list-style-type: none"> <li>• Signatures: <math>SKEYID = sha(Ni\_b   Nr\_b, g^{xy})</math></li> <li>• Pre-shared keys: <math>SKEYID = sha(\text{pre-shared-key}, Ni\_b   Nr\_b)</math></li> <li>• [Authentication using Public key encryption, computing SKEYID as follows: <math>SKEYID = sha(sha(Ni\_b   Nr\_b), CKY-I   Nr\_b)</math></li> </ul>
FCS_IKE_EXT.1.5	The TSF shall compute authenticated keying material as follows: <ul style="list-style-type: none"> <li>• <math>SKEYID\_d = sha(SKEYID, g^{xy}   CKY-I   CKY-R   0)</math></li> <li>• <math>SKEYID\_a = sha(SKEYID, SKEYID\_d   g^{xy}   CKY-I   CKY-R   1)</math></li> <li>• <math>SKEYID\_e = sha(SKEYID, SKEYID\_a   g^{xy}   CKY-I   CKY-R   2)</math></li> <li>• [none]</li> </ul>
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 authorized administrator: <ol style="list-style-type: none"> <li>a) Authentication with digital signatures: The TSF shall use [<i>RSA, "no other digital signature algorithms"</i>]</li> <li>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.</li> <li>c) [<i>X.509 certificates Version 3, [no other versions]</i>] 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.</li> <li>d) Authentication with a pre-shared key: The TSF shall allow authentication using a pre-shared key.</li> </ol>
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)]

## FCS\_IPSEC\_EXT.1 IPSEC

FCS\_IPSEC\_EXT.1.1 The TSF shall implement IPsec using the ESP protocol as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), *[no other algorithms]* and using IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109; *[IKEv2 as defined in RFCs 4306, 4307]* to establish the security association.

FCS\_IPSEC\_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS\_IPSEC\_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

FCS\_IPSEC\_EXT.1.4 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to [200] MB of traffic for Phase 2 SAs.

FCS\_IPSEC\_EXT.1.5 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and *[24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP), [no other DH groups]]*.

FCS\_IPSEC\_EXT.1.6 The TSF shall ensure that all IKE protocols implement Peer Authentication using the *[rDSA]* algorithm.

FCS\_IPSEC\_EXT.1.7 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its IPsec connections.

FCS\_IPSEC\_EXT.1.8 The TSF shall support the following:

1. Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “\*”, “(”, and “)”);
2. Pre-shared keys of 22 characters and [up to 128 characters].

## FCS\_RBG\_EXT.1 Cryptographic operation (random bit generation)

FCS\_RBG\_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with *[FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using 3-Key Triple DES]* seeded by an entropy source that accumulated entropy from at least one independent TSF-hardware-based noise source.

FCS\_RBG\_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [160 bits] of entropy at least equal to the greatest length of the keys and authorization factors that it will generate.

## FCS\_SSH\_EXT.1 SSH

FCS\_SSH\_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS\_SSH\_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed after no more than 2<sup>28</sup> packets have been transmitted using that key.

- FCS\_SSH\_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [*between 1 and 60 minutes*], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [*a maximum number of 3*] attempts.
- FCS\_SSH\_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.
- FCS\_SSH\_EXT.1.5 The TSF shall ensure that, as described in RFC 4253, packets greater than [35,000 bytes] bytes in an SSH transport connection are dropped.
- FCS\_SSH\_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [*no other algorithms*].
- FCS\_SSH\_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH\_RSA and [*no other public key algorithms*] as its public key algorithm(s).
- FCS\_SSH\_EXT.1.8 The TSF shall ensure that data integrity algorithms used in the SSH transport connection is [*hmac-sha1, hmac-sha1-96, hmac-md5, and hmac-md5-96*].
- FCS\_SSH\_EXT.1.9 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

#### FCS\_TLS\_EXT.1 TLS

- FCS\_TLS\_EXT.1.1 The TSF shall implement one or more of the following protocols [*TLS1.0 (RFC 2346)*] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Optional Ciphersuites: [*none*].

### Identification and Authentication (FIA)

#### FIA\_PMG\_EXT.1 Password management

- FIA\_PMG\_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “\*”, “(”, and “)”);
2. Minimum password length shall be settable by the Authorized Administrator, and support passwords of 8 characters or greater;
3. Passwords composition rules specifying the types and number of required characters that comprise the password shall be settable by the Authorized Administrator.
4. Passwords shall have a maximum lifetime, configurable by the Authorized Administrator.
5. New passwords must contain a minimum of 4 character changes from the previous password.

## **FIA\_UAU\_EXT.5 Password-based authentication mechanism**

- FIA\_UAU\_EXT.5.1 The TSF shall provide a local password-based authentication mechanism, *[[remote password-based authentication via RADIUS or TACACS+]]* to perform user authentication.
- FIA\_UAU\_EXT.5.2 The TSF shall ensure that, **when connecting remotely**, users with expired passwords are [locked out until their password is reset by an administrator].

## **Protection of the TSF (FPT)**

### **FPT\_PTD\_EXT.1 Management of TSF data (for reading of authentication data)**

- FPT\_PTD\_EXT.1.1 The TSF shall prevent reading of the plaintext passwords.

### **FPT\_PTD\_EXT.2 Management of TSF data (for reading of all symmetric keys)**

- FPT\_PTD\_EXT.2.1 The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

### **FPT\_TUD\_EXT.1 Trusted update**

- FPT\_TUD\_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.
- FPT\_TUD\_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to the TOE firmware/software.
- FPT\_TUD\_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a *[published hash]* prior to installing those updates.

### **FPT\_TST\_EXT.1 TSF testing**

- FPT\_TST\_EXT.1.1 The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

## **Extended Requirements Rationale**

- FAU\_STG\_EXT.1: This SFR was taken from Protection Profile – Security Requirements for Network Devices, 10 December 2010, Version 1.0 (NDPP) – where it is defined as a requirement to export audit records outside the TOE.
- FAU\_STG\_EXT.3: This SFR was taken from Protection Profile – NDPP – where it is defined as a requirement to detect, and take a defined action, when an external audit server becomes inaccessible.
- FCS\_HTTPS\_EXT.1: This SFR was taken from Protection Profile – NDPP – where it is defined as a requirement specific to HTTPS.
- FCS\_IKE\_EXT.1: This SFR was taken from PD-0105 where IKE is defined as an acceptable instance of single-use authentication.
- FCS\_IPSEC\_EXT.1: This SFR was taken from Protection Profile – NDPP – where it is defined as a requirement specific to IPSEC.
- FCS\_RBG\_EXT.1: This SFR was taken from Protection Profile – NDPP – where it is defined as a requirement specific to random bit generation.
- FCS\_SSH\_EXT.1: This SFR was taken from Protection Profile – NDPP – where it is defined as a requirement specific to SSH.
- FCS\_TLS\_EXT.1: This SFR was taken from Protection Profile – NDPP – where it is defined as a requirement specific to TLS.
- FIA\_PMG\_EXT.1: This SFR was taken from Protection Profile – NDPP – where it is defined as a requirement for specific password composition and aging constraints. Note

that “Security Administrator” has been replaced with “Authorized Administrator”.

- FIA\_UAU\_EXT.5: This SFR was taken from Protection Profile – NDPP – where it is defined as a requirement allowing the identification of required external authentication services.
- FPT\_PTD\_EXT.1: This SFR was taken from Protection Profile – NDPP (as FPT\_PTD.1(1)) – where it is defined as a requirement specifically disallowing access to identified TSF data.
- FPT\_PTD\_EXT.2: This SFR was taken from Protection Profile – NDPP (as FPT\_PTD.1(2)) – where it is defined as a requirement specifically disallowing access to identified TSF data.
- FPT\_TST\_EXT.1: This SFR was taken from Protection Profile – NDPP – where it is defined as a requirement for TSF self tests during initialization.
- FPT\_TUD\_EXT.1: This SFR was taken from Protection Profile – NDPP – where it is defined as a requirement for secure TOE update capabilities. Note that “Security Administrator” has been replaced with “Authorized Administrator”.

**Summary of representation of SFRs from the Network Device Protection Profile (NDPPv1.0):**

[Note: This ST does not claim conformance to the NDPP.]

SFR from NDPP	Representation in this ST
FAU_GEN.1	Redundant to FWPP.
FAU_GEN.2	Added to this ST.
FAU_STG_EXT.1	Added to this ST.
FAU_STG_EXT.3	Added to this ST.
FCS_CKM.1	Added to this ST.
FCS_CKM_EXT.4	Added to this ST as FCS_CKM.4.
FCS_COP.1(1)	Added to this ST.
FCS_COP.1(2)	Added to this ST as FCS_COP.1(3).
FCS_COP.1(3)	Added to this ST as FCS_COP.1(4).
FCS_COP.1(4)	Added to this ST as FCS_COP.1(2).
FCS_HTTPS_EXT.1	Added to this ST.
FCS_IPSEC_EXT.1	Added to this ST.
FCS_RBG_EXT.1	Added to this ST.
FCS_SSH_EXT.1	Added to this ST.
FCS_TLS_EXT.1	Added to this ST.
FCS_COMM_PROT_EXT.1	Redundant to iterations of FTP_ITC, and FTP_TRP.
FDP_RIP.2	Added to this ST, superseding FDP_RIP.1 from FWPP.
FIA_PMG_EXT.1	Added to this ST.
FIA_UIA_EXT.1	Redundant to FIA_UID.2 from FWPP.
FIA_UAU_EXT.5	Added to this ST. This iteration differs from FIA_UAU.5 (from FWPP) in that this iteration is specific to password expiration.
FIA_UAU.6	Added to this ST.
FIA_UAU.7	Added to this ST.
FMT_MTD.1	Added to this ST as FMT_MTD.1(1) and FMT_MTD.1(2).
FMT_SMF.1	Added to this ST.
FMT_SMR.1	Redundant to FMT_SMR.1 from FWPP.
FPT_ITT.1(1)	Added to this ST as FPT_ITT.1.

FPT_ITT.1(2)	Added to this ST merged with FPT_ITT.1.
FPT_PTD.1(1)	Added to this ST.
FPT_PTD.1(2)	Added to this ST.
FPT_RPL.1	Added to this ST.
FPT_STM.1	Redundant to FPT_STM.1 from FWPP.
FPT_TUD_EXT.1	Added to this ST.
FPT_TST_EXT.1	Added to this ST.
FRU_RSA.1	Added to this ST.
FTA_SSL_EXT.1	Merged with FTA_SSL.3 from NDPP.
FTA_SSL.3	Added to this ST.
FTA_TAB.1	Added to this ST.
FTP_ITC.1(1)	Added to this ST.
FTP_ITC.1(2)	Added to this ST.
FTP_TRP.1(1)	Added to this ST.
FTP_TRP.1(2)	Added to this ST.

## 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_GEN.2	FAU_GEN.1 FIA_UID.1	Met by FAU_GEN. Met by FIA_UID.2
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), and (4)  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), and (4)  Met by FCS_CKM.4
FCS_CKM.1(3)	FCS_CKM.2 or FCS_COP.1	Met by FCS_COP.1(2), (3), and (4)

SFR	Dependency	Rationale
	FCS_CKM.4	Met by FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Met by 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 (3) Met by FCS_CKM.4
FCS_COP.1(4)	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)

<b>SFR</b>	<b>Dependency</b>	<b>Rationale</b>
FDP_RIP.2	No dependencies	N/A
FIA_AFL.1	FIA_UAU.1	Met by FIA_UAU.1
FIA_ATD.1	No dependencies	N/A
FIA_UAU.1	FIA_UID.1	Met by FIA_UID.2
FIA_UAU.5	No dependencies	N/A
FIA_UAU.6	No dependencies	N/A
FIA_UAU.7	FIA_UAU.1	Met by FIA_UID.2
FIA_UID.2	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

<b>SFR</b>	<b>Dependency</b>	<b>Rationale</b>
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
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_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	Met by FIA_UID.2
FPT_ITT.1	No dependencies	N/A
FPT_RPL.1	No dependencies	N/A
FPT_STM.1	No dependencies	N/A
FRU_RSA.1	No dependencies	N/A
FTA_SSL.3	No dependencies	N/A
FTA_TAB.1	No dependencies	N/A
FTP_ITC.1(1)	No dependencies	N/A
FTP_ITC.1(2)	No dependencies	N/A
FTP_TRP.1(1)	No dependencies	N/A
FTP_TRP.1(2)	No dependencies	N/A
FAU_STG_EXT.1	FAU_GEN.1	Met by FAU_GEN.1

SFR	Dependency	Rationale
FAU_STG_EXT.3	FAU_STG_EXT.1	Met by FAU_STG_EXT.1
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	Met by FCS_TLS_EXT.1
FCS_IKE_EXT.1	None required by PD-0105.	Supported by FCS_RBG_EXT.1
FCS_IPSEC_EXT.1	FCS_COP.1	FCS_COP.1(*)
FCS_RBG_EXT.1	No dependencies	N/A
FCS_SSH_EXT.1	FCS_COP.1	FCS_COP.1(*)
FCS_TLS_EXT.1	FCS_COP.1	FCS_COP.1(*)
FIA_PMG_EXT.1	No dependencies	N/A
FIA_UAU_EXT.5	No dependencies	N/A
FPT_PTD_EXT.1	No dependencies	N/A
FPT_PTD_EXT.2	No dependencies	N/A
FPT_TST_EXT.1	No dependencies	N/A
FPT_TUD_EXT.1	No dependencies	N/A

## 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 3. 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 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

Assurance Class	Components	Components Description
	ALC_TAT.1	Well-defined development tools
	ALC_FLR.2	Flaw Reporting Procedures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: basic design
	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 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

<b>Component</b>	<b>How the requirement will be met</b>
	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 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**

TOE SFRs	How the SFR is Met																
FAU_GEN.1	<p>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.</p> <p>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.</p> <table border="1" data-bbox="440 720 1438 1850"> <thead> <tr> <th data-bbox="440 720 808 768">Auditable Event</th> <th data-bbox="808 720 1438 768">Rationale</th> </tr> </thead> <tbody> <tr> <td data-bbox="440 768 808 1031">Modifications to the group of users that are part of the authorized administrator role.</td> <td data-bbox="808 768 1438 1031">All changes to the configuration (and hence all security relevant administrator actions) 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 data-bbox="440 1031 808 1136">All use of the user identification mechanism.</td> <td data-bbox="808 1031 1438 1136">Events will be generated for attempted identification/authentication, and the username attempting to authenticate will be recorded in the event.</td> </tr> <tr> <td data-bbox="440 1136 808 1276">Any use of the authentication mechanism.</td> <td data-bbox="808 1136 1438 1276">Events will be generated for attempted identification/authentication, and the username attempting to authenticate will be recorded in the event along with the origin or source of the attempt.</td> </tr> <tr> <td data-bbox="440 1276 808 1507">The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the user's capability to authenticate.</td> <td data-bbox="808 1276 1438 1507">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. Changes to restore a locked account would fall into the category of configuration changes.</td> </tr> <tr> <td data-bbox="440 1507 808 1675">All decisions on requests for information flow.</td> <td data-bbox="808 1507 1438 1675">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.</td> </tr> <tr> <td data-bbox="440 1675 808 1843">Success and failure, and the type of cryptographic operation</td> <td data-bbox="808 1675 1438 1843">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.</td> </tr> <tr> <td data-bbox="440 1843 808 1890">Changes to the time.</td> <td data-bbox="808 1843 1438 1890">Changes to the time are logged.</td> </tr> </tbody> </table>	Auditable Event	Rationale	Modifications to the group of users that are part of the authorized administrator role.	All changes to the configuration (and hence all security relevant administrator actions) 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.	All use of the user identification mechanism.	Events will be generated for attempted identification/authentication, and the username attempting to authenticate will be recorded in the event.	Any use of the authentication mechanism.	Events will be generated for attempted identification/authentication, and the username attempting to authenticate will be recorded in the event along with the origin or source of the attempt.	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the user's capability to authenticate.	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. 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.
Auditable Event	Rationale																
Modifications to the group of users that are part of the authorized administrator role.	All changes to the configuration (and hence all security relevant administrator actions) 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.																
All use of the user identification mechanism.	Events will be generated for attempted identification/authentication, and the username attempting to authenticate will be recorded in the event.																
Any use of the authentication mechanism.	Events will be generated for attempted identification/authentication, and the username attempting to authenticate will be recorded in the event along with the origin or source of the attempt.																
The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the user's capability to authenticate.	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. 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.																

TOE SFRs	How the SFR is Met	
	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.
	Loss of connectivity with an external syslog server.	Loss of connectivity with an external syslog server is logged as a terminated or failed cryptographic channel.
	Initiation of an update to the TOE.	TOE updates are logged as configuration changes.
	Termination of a remote session. Note that the TOE does not support session locking, so there is no corresponding audit.	Termination of a remote session is log as a terminated cryptographic path.
	Initiation, termination and failures in trusted channels and paths.	Requests for encrypted session negotiation are logged (whether successful or failed). Similarly, when an established cryptographic channel or path is terminated or fails a log record is generated.
FAU_GEN.2	The ASA ensures each action performed by the administrator at the CLI is logged with the administrator's identity and as a result they are traceable to a specific user.	
FAU_SAR.1	<p>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'.</p> <p>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.</p>	
FAU_SAR.3	<p>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:</p> <ul style="list-style-type: none"> <li>• Severity</li> <li>• Date</li> <li>• Time</li> <li>• Syslog ID</li> <li>• Source ID (User Identity)</li> </ul>	

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> <li>• Source (Presumed subject address)</li> <li>• Destination ID</li> <li>• Destination (address/ Presumed subject address)</li> </ul> <p>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).</p> <p>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.</p>
FAU_STG.1	<p>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.</p>
FAU_STG.4	<p>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.</p> <p>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.</p>
FCS_CKM.1(1) through (3), FCS_CKM.4, FCS_COP.1(1) through (4), and FCS_RBG_EXT.1	<p>The ASA uses a FIPS validated implementation of AES with 128, 192, and 256 bit keys. Satisfying P.CRYPTO, all the ASA models in the TOE implement AES in hardware using the Cavium Nitrox Lite (FIPS validations #105, #564, #1394, and #1407, relevant to FIPS 140-2 Cert# 1436 for all ASA models in the TOE). Configuring the ASA software in or out of FIPS mode does not modify the ASA’s use of the FIPS-validated AES through implementation of the Cavium Nitrox Lite. AES is used in CBC mode (as described in NIST SP 800-38A) and three key Triple-DES with 168 bit keys.</p> <p>The ASA implements a random number generator (RNG) that meets ANSI X9.31 and is based on the RSA key establishment schemes, as specified in NIST SP 800-56B “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”.</p> <p>The ASA meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs).</p> <p>The ASA provides cryptographic hashing services using SHA-1 or SHA-2 and keyed-hash message authentication using HMAC-SHA-1 with 160-bit key sizes.</p> <p>The ASA provides cryptographic signature services using RSA with key sizes (modulus) of 1024 or 2048 bits. The key size is configurable.</p> <p>In the ASA cryptographic functions are used to establish TLS, HTTPS, and SSH sessions, for IPSec traffic and authentication keys, and for IKE authentication and encryption keys.</p>
FDP_IFC.1(1) and FDP_IFF.1(1)	<p>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:</p> <ul style="list-style-type: none"> <li>• presumed address of source</li> </ul>

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> <li>• presumed address of destination</li> <li>• transport layer protocol</li> <li>• Service used</li> <li>• Network interface on which the connection request occurs</li> </ul> <p>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.</p> <p>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 &gt; Firewall &gt; Access Rules’ screen.</p> <p>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.</p>
FDP_IFC.1(2) and FDP_IFF.1(2)	<p>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:</p> <ul style="list-style-type: none"> <li>• User identity</li> <li>• presumed address of source</li> <li>• presumed address of destination</li> <li>• transport layer protocol</li> <li>• Service used</li> <li>• Security-relevant service command</li> <li>• Network interface on which the connection request occurs</li> </ul> <p>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.</p> <p>Telnet and FTP traffic can be forced to authenticate.</p> <p>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 &gt; Firewall &gt; Access Rules’ screen.</p> <p>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.</p>
FDP_IFC.1(3) and FDP_IFF.1(3)	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• User identity</li> </ul>

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> <li>• Presumed address of source</li> <li>• Presumed address of destination</li> </ul> <p>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.</p> <p>These policies are created in the form of crypto policies at the CLI (via ‘crypto map’ commands) or via ASDM on the ‘Configuration &gt; Remote Access VPN’ and ‘Configuration &gt; Site-to-Site VPN’ pages.</p> <p>The TOE will take the following actions based on the VPN policy:</p> <ul style="list-style-type: none"> <li>• pass packets without modifying;</li> <li>• send IPSEC encrypted and authenticated packets to a VPN peer using ESP in tunnel mode as defined in RFC 2406;</li> <li>• send TLS encrypted and authenticated packets to a VPN peer over an HTTPS tunnel;</li> <li>• decrypt, verify authentication and pass received packets from a VPN peer in tunnel mode using ESP;</li> <li>• decrypt, verify authentication and pass received packets from a VPN peer in tunnel mode using TLS handshake;</li> </ul> <p>Note: the TOE does not support IPv6 IPsec VPNs. The TOE only supports IPsec VPN via IPv4.</p>
FDP_IFC.1(4) and FDP_IFF.1(4)	<p>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.</p> <p>The ASA 5510, 5520, 5540, 5550, 5580, and 5585 do not come preconfigured with any VLANs, however their physical ports can be divided into sub-interfaces using an option on the ‘interface’ command.</p> <p>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.</p>
FDP_RIP.2	<p>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.</p>
FIA_AFL.1	<p>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 &gt; Device Management &gt; Users/AAA &gt; AAA Server Groups’ page). The number of failures to be detected and trigger the lockout can be between 1 and 16. Administrative accounts with privilege level 15 are exempt from lockout due to successive failed</p>

TOE SFRs	How the SFR is Met
	<p>login attempts. To enforce the ability to lockout any local account after consecutive failed logins, administrators ensure that no privilege level 15 accounts exist in the local user database, and require administrators to use the “enable” command to activate the level 15 privileges after successfully authenticating.</p> <p>NOTE: All accounts (administrators and VPN users) that are authenticated to the remote AAA server and not to the local ASA user database will not be subjected to the account lockout function of the ASA. When account authentication is deferred to a remote AAA server the remote AAA server is expected to enforce account lockout due to consecutive failed login attempts. The TOE administrator can define which authentication mechanism are used for each interface (e.g. whether to use remote AAA or LOCAL, or to allow fallback from remote AAA to LOCAL for each of serial, SSH, or ASDM).</p> <p>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).</p>
FIA_ATD.1	<p>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 &gt; Device Management &gt; Users/AAA &gt; 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.</p>
FIA_UAU.5.1 and FIA_UAU_EXT.5	<p>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.</p> <p>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 &gt; Device Management &gt; Users/AAA &gt; AAA Server Groups’ and ‘Configuration &gt; Device Management &gt; Users/AAA &gt; AAA Access &gt; Authentication’ pages respectively.</p> <p><b>NOTE:</b> 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.</p> <p>In the case of users defined on an external authentication server, if the user’s password expires the user will not be able to log in until they either change their password in accordance with the requirements of the external authentication server or an administrator intervenes to correct the situation.</p>
FIA_UAU.6	Users changing their passwords are first prompted to enter their old password.
FIA_UAU.7	When a user enters their password at the local console, the ASA displays only ‘*’ characters so that the user password is obscured. For remote session authentication, the ASA does not echo any characters as they are entered.
FIA_UID.2, 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 user 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

TOE SFRs	How the SFR is Met
	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)	<p>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:</p> <p>enable: 'logging enable'; disable: 'no logging enable'; determine/ modify: 'show config', 'logging', 'clear logging buffer'; review: 'show logging'</p> <p>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'</p> <p>'ssh' (use 'interface' keyword to specify/ limit interfaces); '(no) snmp server'; '(no) telnet'; 'http server enable'; 'http' (with the 'interface' keyword)</p> <p>The ASDM uses the same privileges that the user would have at the CLI to determine access to administrative functions in the ASDM GUI.</p>
FMT_MSA.1(1) through FMT_MSA.1(8)	<p>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.</p> <p>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.</p>
FMT_MSA.2	When the VPN clients are configured in FIPS mode, the defined encryption functions will not operate with key sizes or algorithms that are not FIPS compliant. The ASA will only accept cryptographic parameters that the administrator explicitly enables for peer-to-peer VPNs, and client VPNs.
FMT_MSA.3(1) and FMT_MSA.3(2)	<p>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.</p> <p>The ASA 5505 comes preconfigured with two VLANs: VLAN1 and VLAN2. The ASA 5510, 5520, 5540, 5550, 5580, and 5585 do not come preconfigured with any VLANs. Regardless of the out-of-the-box configuration, the TOE enforces restrictive default values for information with respect to VLANs in that whenever VLANs are configured, the default behavior of the TOE is to restrict traffic flow of any VLAN to remain among ports assigned to that VLAN and isolated from all other traffic flows. The administrator can specify alternative initial values by configuring additional VLANs, reassigning VLANs to non-default interfaces, configuring VLAN trunks, or by explicitly allowing Layer 3 traffic (with IP addressing) to be routed out of any VLAN to other VLANs or to non-VLAN networks as permitted by the</p>

TOE SFRs	How the SFR is Met
	UNAUTHENTICATED_SFP, the AUTHENTICATED_SFP, or the VPN_SFP.
FMT_MTD.1(1), FMT_MTD.1(2) and FMT_MTD.2	<p>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.</p> <p>The ASDM uses the same privileges that the user would have at the CLI to determine access to administrative functions in the ASDM GUI.</p>
FMT_SMF.1	<p>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.</p> <p>Note that the ASA does not provide services (other than connecting using SSH, HTTPS, and establishment of VPNs) prior to authentication so there are no applicable comments. There are specific commands for the configuration of cryptographic services. Trusted updates to the product can be verified using cryptographic checksum (i.e., a published hash).</p> <p>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.</p>
FMT_SMR.1	<p>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 with full read-write access. 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 &gt; Device Management &gt; Users/AAA &gt; User Accounts' page.</p> <p>Usernames defined within the local user database are distinguished based on their privilege level (0-15) and the service-type attribute assigned to the username, which by default it "admin", allowing the username to authenticate (with valid password) to admin interfaces.</p> <p>'aaa authentication ssh console LOCAL' can be used to set the ASA to authenticate SSH users against the local database.</p> <p>'aaa authorization exec' can be used to require re-authentication of users before they can get to EXEC mode.</p> <p>The ASA also supports creating of VPN User accounts, which cannot login locally to the ASA, but can only authenticate VPN sessions initiated from VPN Clients. VPN users are accounts with privilege level 0, and/or with their service-type attribute set to "remote-access".</p> <p>When command authorization has been enabled the default sets of privileges take effect at certain levels, and the levels become customizable.</p> <ul style="list-style-type: none"> <li>• When "aaa authorization command LOCAL" has NOT been applied to the config:</li> </ul>

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> <li>○ All usernames with level 2 and higher have the same full read-write access as if they had level 15 once their interactive session (CLI or ASDM) is effectively at level 2 or higher.</li> <li>○ Usernames with privilege levels 1 and higher can login to the CLI, and “enable” to their max privilege level (the level assigned to their username).</li> <li>○ Usernames with privilege levels 2-14 can login to ASDM, and have full read-write access.</li> <li>○ Privilege levels cannot be customized.</li> <li>• When “aaa authorization command LOCAL” has been applied to the config: <ul style="list-style-type: none"> <li>○ Default command authorizations for privilege levels 3 and 5 take effect, where level 3 provides “Monitor Only” privileges, levels 4 and higher inherit privileges from level 3, level 5 provides “Read Only” privileges (a superset of Monitor Only privileges), and levels 6-14 inherit privileges from level 5.</li> <li>○ Privilege levels (including levels 3 and 5) can be customized from the default to add/remove specific privileges.</li> <li>○ To display the set of privileges assigned to levels 3 or 5 (or any other privilege level), use “show running-config all privilege all”, which shows all the default configuration settings that are not shown in the output of “show running-config all”.</li> </ul> </li> </ul>
FPT_ITT.1	<p>The communication between the ASA and the ASDM is protected (from disclosure and modification) via HTTPS session. This protects the data from disclosure by encryption within the TLSv1 protocol, and by checksums that verify that data has not been modified.</p> <p>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.</p>
FPT_RPL.1	<p>By virtue of the cryptographic channel and path mechanisms implemented by ASA, and replayed network packets directed at the ASA will be detected and discarded.</p> <p>Note: The intended scope of this requirement is trusted communications with the ASA (e.g., administrator to ASA, IT entity (e.g., syslog server) to ASA, ASDM to ASA). As such, it does not apply to receipt of multiple network packets due to network congestion or lost packet acknowledgments.</p>
FPT_STM.1	<p>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.</p> <p>This functionality can be set at the CLI using the ‘clock’ commands or in ASDM through the ‘Configuration &gt; Device Setup &gt; System Time’ page. The TOE can optionally be set to receive time from an NTP server.</p>
FRU_RSA.1	<p>An administrator can configure a maximum number of concurrent sessions for remote administrative interfaces.</p>
FTA_SSL.3	<p>An administrator can configure maximum inactivity times for both local and remote administrative sessions. When a session is inactive (i.e., not session input) for the configured period of time the ASA will terminate the session, requiring the administrator to log in again to establish a new session when needed.</p>

TOE SFRs	How the SFR is Met
FTA_TAB.1	<p>The ASA provides administrators with the capability to configure advisory banner or warning message(s) that will be displayed prior to completion of the logon process to VPN users (via AyConnect and Cisco VPN Client) and/or ASA administrators in at the local console or via a remote connection. As such, they can decide whether to continue to log in after reviewing the configured messages.</p>
FTP_ITC.1(1) and FTP_ITC.1(2)	<p>The ASA protects (i.e., from disclose and modification) the certificate traffic between the ASA and other Certificate Authorities using OCSPs. The ASA uses a local CA feature for revocation checking using OCSP when validating the client certificate.</p> <p>The ASA also protects communications with a remote syslog server via SSL. The ASA uses SSLv3.1, DTLS and TLSv1 to provide a secure connection between remote users and specific, supported internal resources as configured by the administrator.</p> <p>IPSec is used by the ASA to establish secure VPN connections with client and gateway peers.</p>
FTP_TRP.1(1) and FTP_TRP.1(2)	<p>The ASA uses SSHv2 or TLS/HTTPS (for ASDM) to provide the trusted path (with protection from disclosure and modification) for all remote administration sessions.</p>
FAU_STG_EXT.1 and FAU_STG_EXT.3	<p>The ASA can be configured export syslog records to a specified, external syslog server. The ASA protects communications with an external syslog server via SSL.</p> <p>If the SSL connection fails, the ASA can be configured such that it will block any new ‘permit’ actions that might occur. In other words, it can be configured to stop forwarding network traffic when it discovers it can no longer communicate with its configured syslog server.</p>
FCS_HTTPS_EXT.1	<p>The ASA implements HTTPS in accordance with RFC 2818 using its implementation of TLS as specified in FCS_TLS_EXT.1.</p>
FCS_IKE_EXT.1	<p>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.</p> <p>IPSec Internet Key Exchange (v1 and v2), 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:</p> <ul style="list-style-type: none"> <li>• The negotiation of mutually acceptable IPSec options between peers,</li> <li>• The establishment of additional Security Associations to protect packets flows using ESP, and</li> <li>• The agreement of secure bulk data encryption Triple-DES (168-bit) /AES (128, 192 or 256 bit) keys for use with ESP.</li> </ul> <p>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 policies 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</p>

TOE SFRs	How the SFR is Met
	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
FCS_IPSEC_EXT.1	<p>The ASA implements IPsec using the ESP protocol as defined by RFC 4303, using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), and using IKEv1 and IKEv2, as specified for FCS_IKE_EXT.1, to establish security associations.</p> <p>The IKE Phase 1 exchanges use only main mode and the IKE SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs. Furthermore, the IKE SA lifetime limits can be configured so that no more than 200 MB of traffic can be exchanged for Phase 2 SAs.</p> <p>The IKE protocols supported by the ASA implement the following DH groups: 14 (2048-bit MODP), 24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), and 20 (384-bit Random EC) and use the rDSA algorithm for Peer Authentication.</p> <p>Pre-shared keys can be configured in ASA for IPsec connection authentication. However, pre-shared keys are only supported when using IKEv2 for peer-to-peer VPNs and when using IKEv1 for remote access VPNs. The pre-shared keys can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “)”) and can be at least 22 characters in length.</p>
FCS_RBG_EXT.1	<p>The ASA implements a random bit generator (RBG) based on the AES-256 block cipher, as specified in FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4. The ASA uses the following Cavium chips: CN505, CN1010, CN1520, CN1610, and CN1620. Versions of the CN1010, CN1520, CN1610 and CN1620 have been FIPS 140-2 validated. Specific hardware and firmware versions are identified on the FIPS 140-2 validation list. The relevant certificate numbers are #870/#871 (CN1010), #1360/#1361 (CN1520), and #1369/#1511 (CN1610,</p>

TOE SFRs	How the SFR is Met
	CN1620).
FCS_SSH_EXT.1	The ASA implements SSHv2 in accordance with RFCs 4251, 4252, 4253, and 4254. SSHv2 sessions are limited to a configurable session timeout period from 1 to 60 minutes, a maximum number of failed authentication attempts limited to 3, and a maximum transmission of 2 <sup>28</sup> packets before the SSH connection must be rekeyed. SSH connections will be dropped if the ASA receives a packet larger than 35,000 bytes. ASA's implementation of SSHv2 supports hashing algorithms hmac-sha1, hmac-sha1-96, hmac-md5, and hmac-md5-96.
FCS_TLS_EXT.1	The ASA implements TLSv1 in accordance with RFC 2346 with the following ciphersuites: <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> <li>• TLS_DHE_RSA_WITH_AES_128_CBC_SHA</li> <li>• TLS_DHE_RSA_WITH_AES_256_CBC_SHA.</li> </ul>
FIA_PMG_EXT.1	The ASA supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, and “)”. Minimum password length is settable by the Authorized Administrator, and support passwords of 8 characters or greater. Password composition rules specifying the types and number of required characters that comprise the password are settable by the Authorized Administrator. Passwords have a maximum lifetime, configurable by the Authorized Administrator. New passwords must contain a minimum of 4 character changes from the previous password.  Password complexity settings, minimum password length, and requiring a minimum number of character changes from previous password, are not enforced by the “username” command (when an authenticated privileged administrator is modifying the password for another administrator or him/herself without using the “change-password” command), and are only enforced: <ol style="list-style-type: none"> <li>1. When an admin is forced to change his/her own password at login, such as when the password lifetime has expired.</li> <li>2. When using the “change-password” command to change one’s own password after login.</li> </ol> NOTE: All accounts (administrators and VPN users) that are managed within a remote AAA server and not to the local ASA user database will not have password complexity controls enforced by the ASA. When remote AAA servers are used to manage accounts, those servers would be the enforcement point for password complexity controls.
FPT_PTD_EXT.1 and FPT_PTD_EXT.2	The ASA includes a Master Passphrase features that can be used to configure the ASA to encrypt all locally defined user passwords. In this manner, the ASA ensures that plaintext user passwords will not be disclosed even to administrators.  The ASA stores all private keys in a secure directory that is not readily accessible to administrators. All pre-shared and symmetric keys are stored in encrypted form to prevent access.
FPT_TST_EXT.1	The ASA runs a suite of self tests during initial start-up (power-on-self-tests) to verify its correct operation. When FIPS mode is optionally enabled on the ASA, additional cryptographic tests will be run during start-up.
FPT_TUD_EXT.1	The ASA (and other TOE components) have specific versions that can be queried by an administrator. When updates are made available by Cisco, an administrator can obtain and install those updates.

TOE SFRs	How the SFR is Met
	Cryptographic checksums (i.e., public hashes) are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components.

## 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.ENHEXP	T.UNAUTHPEER	T.UNTRUSTPATH	T.VLAN	T.ADMIN_ERROR	T.RESOURCE_EXHAUSTION	T.TSF_FAILURE	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.UNDETECTED_ACTIONS	T.USER_DATA_REUSE	P.CRYPTO	P.INTEGRITY	P.ACCESS_BANNER
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.INGTEGRITY													X										X	
O.KEYCONF													X											
O.PEERAUTH												X												
O.VLAN														X										
O.DISPLAY_BANNER																								X
O.PROTECTED_COMMUNICATIONS																		X						
O.RESIDUAL_INFORMATION_CLEARING																					X			
O.RESOURCE_AVAILABILITY																X								
O.SESSION_LOCK																		X						
O.SYSTEM_MONITORING															X			X	X					
O.TOE_ADMINISTRATION																		X						



O.PEERAUTH This security objective is necessary to counter the threat T.UNAUTHPEER because it ensures that remote VPN endpoints (clients and gateways) must be authenticated to the TOE using strong authentication 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.

O.DISPLAY\_BANNER This security objective is necessary to address the policy P.ACCESS\_BANNER because it ensures an advisory banner is displayed when users log in to establish interactive sessions.

O.PROTECTED\_COMMUNICATIONS This security objective is necessary to counter the threat T.UNAUTHORIZED\_ACCESS because it ensures the TOE will properly encrypt its communication channels to protect them.

O.RESIDUAL\_INFORMATION\_CLEARING This security objective is necessary to counter the threat T.USER\_DATA\_REUSE because it ensures the TOE will properly manage resources to ensure objects are not formed from resources that may have residual data.

O.RESOURCE\_AVAILABILITY This security objective is necessary to counter the threat T.RESOURCE\_EXHAUSTION because it ensures the TOE implements mechanisms that will meter critical resources to mitigate the possibility of resource exhaustion.

O.SESSION\_LOCK This security objective is necessary to counter the threat T.UNAUTHORIZED\_ACCESS because it ensures the TOE will lock inactive, and hence perhaps unattended, interactive sessions.

O.SYSTEM\_MONITORING This security objective is necessary to counter the threats T.ADMIN\_ERROR, T.UNAUTHORIZED\_ACCESS, and T.UNDETECTED\_ACTIONS because it ensures the TOE will log administrator commands that might serve to help identify previous errors and the TOE will log security relevant events that might be indicative of inappropriate access or access that requires accountability.

O.TOE\_ADMINISTRATION This security objective is necessary to counter the threat T.UNAUTHORIZED\_ACCESS because it ensures the TOE is designed to ensure that only administrators can access security management functions and only after they have been properly identified and authenticated.

O.TSF\_SELF\_TEST This security objective is necessary to counter the threat T.TSF\_FAILURE because it ensures the TOE includes self-tests to ensure that it is working correctly.

O.VERIFIABLE\_UPDATES This security objective is necessary to counter the threat T.UNAUTHORIZED\_UPDATE because it ensures the TOE includes mechanisms to verify the source and integrity of updates prior to their use.

## 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 hardware component of the TOE is physically secure.

OE.ENHEXP 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.INGTEGRITY	O.KEYCONF	O.PEERAUTH	O.VLAN	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.RESOURCE_AVAILABILITY	O.SESSION_LOCK	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST	O.VERIFIABLE_UPDATES
FAU_GEN.1							X	X														X			
FAU_GEN.2																						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.1(3)																	X								
FCS_CKM.4													X												
FCS_COP.1(1)					X						X	X													
FCS_COP.1(2)											X	X					X								
FCS_COP.1(3)											X	X					X							X	
FCS_COP.1(4)											X						X							X	
FDP_IFC.1(1)			X																						
FDP_IFC.1(2)			X																						
FDP_IFC.1(3)					X							X	X												
FDP_IFC.1(4)																X									
FDP_IFF.1(1)			X																						
FDP_IFF.1(2)			X																						
FDP_IFF.1(3)					X							X	X												
FDP_IFF.1(4)																X									
FDP_RIP.2			X															X							
FIA_AFL.1						X																			
FIA_ATD.1	X								X																





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.1 Cryptographic key generation (3)

This component ensures that the TSF is able to generate encryption keys to support other cryptographic operations. This traces back to and aids in meeting the following objective: O.PROTECTED\_COMMUNICATIONS.

FCS\_CKM.4 Cryptographic key destruction

This component ensures that keys used for encryption and signatures are destroyed when no longer needed by overwriting with zeros. This component traces back to and aids in meeting the following objective: O.KEYCONF.

FCS\_COP.1 Cryptographic operation (1)

This component ensures that since the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that 3DES and FIPS-conformant AES are 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.ENCRYPT, O.INTEGRITY, and O.EAL.

FCS\_COP.1 Cryptographic operation (2)

This component ensures that the TSF will implement FIPS-conformant HMAC SHA-1, SHA-256, SHA-384, and/or SHA-512 in support of cryptographic protocols. This traces back to and aids in meeting the following objective: O.PROTECTED\_COMMUNICATIONS, and O.EAL.

FCS\_COP.1 Cryptographic operation (2) and (3)

These components ensure that a message authentication code is generated and used therefore its authenticity can be established cryptographically. They also support the protected communication with the CA to check that the digital certificate is trustworthy. These components trace back to and aids in meeting the following objective: O.TRUSTEDPATH, and O.EAL.

FCS\_COP.1 Cryptographic operation (3)

This component ensures that the TSF will implement FIPS-conformant DSA, rDSA, and/or ECDSA in support of cryptographic protocol. This traces back to and aids in meeting the following objective: O.PROTECTED\_COMMUNICATIONS, and O.EAL.

FCS\_COP.1 Cryptographic operation (3) and (4)

These components ensure that a the TSF either uses digital signatures or cryptographic hashes to ensure the integrity of updates. These components trace back to and aids in meeting the following objective: O.VERIFIABLE\_UPDATES.

FCS\_COP.1 Cryptographic operation (4)

This component ensures that the TSF will implement FIPS-conformant SHA-1, SHA-256, SHA-384, and/or SHA-512 in support of cryptographic protocols. This traces back to and aids in meeting the following objective: O.PROTECTED\_COMMUNICATIONS, and O.EAL.

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, O.ENCRYP, 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, O.ENCRYP, 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.2 Full 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 objectives: O.MEDIAT and O.RESIDUAL\_INFORMATION\_CLEARING.

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\_UAU.6 Re-authenticating

This component ensures that the TSF will ensure that users must be re-authenticated in order to change their password to further ensure the user changing the password is authentic. This traces back to and aids in meeting the following objective: O.TOE\_ADMINISTRATION.

#### FIA\_UAU.7 Protected Authentication Feedback

This component ensures that the TSF will not echo passwords when being entered to mitigate the chance of an accidental password disclosure s. This traces back to and aids in meeting the following objective: O.TOE\_ADMINISTRATION.

#### 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\_IFF.1(3). This component traces back to and aids in meeting the following objectives: O.TRUSTEDPATH, O.INTEGRITY, 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.TRUSTEDPATH, O.INTEGRITY, 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, delete, or modify rules attributes listed in FDP\_IFF.1(4). This component traces back to and aids in meeting the following objectives: O.VLAN, 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 that are listed in FDP\_IFF.1(4). This component traces back to and aids in meeting the following objectives: O.SECSTA, O.VLAN, 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.VLAN 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. It also ensures that the TSF will provide a minimum set of security functions to ensure the TOE security features can be properly managed. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.TOE\_ADMINISTRATION.

#### 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). It also ensures that the TSF will provide a minimum set of a Administrator roles and can implement additional roles where necessary. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.TOE\_ADMINISTRATION.

#### 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 objectives: O.ENCRYP and O.PROTECTED\_COMMUNICATIONS.

#### FPT\_RPL.1 Replay Detection

This component ensures that the TSF will prevent the replay of data to ensure that data cannot be collected and reused at some later time to benefit an attacker. This traces back to and aids in meeting the following objective: O.PROTECTED\_COMMUNICATIONS.

#### 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 objectives: O.AUDREC and O.SYSTEM\_MONITORING.

#### FRU\_RSA.1 Maximum Quotas

This component ensures that the TSF will enforce resource quotas for defined resources to reduce the potential for critical resource exhaustion. This traces back to and aids in meeting the following objective: O.RESOURCE\_AVAILABILITY.

#### FTA\_SSL.3 TSF-initiated Termination

This component ensures that the TSF will terminate local and remote sessions after an administrator defined period of inactivity indicating the user may not be in attendance. This traces back to and aids in meeting the following objectives: O.SESSION\_LOCK and O.TOE\_ADMINISTRATION.

#### FTA\_TAB.1 Default TOE Access Banners

This component ensures that the TSF will display a configured advisory banner whenever a user/administrator connects to the TOE. This traces back to and aids in meeting the following objective: O.DISPLAY\_BANNER.

#### FTP\_ITC.1 Basic internal TSF data transfer protection (1) and (2)

These components ensure 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, O.SELPRO, and O.PROTECTED\_COMMUNICATIONS.

#### FTP\_TRP.1 Trusted Path (1) and (2)

These components ensure that the TSF will protect communication between itself and its administrators from disclosure and modification. These trace back to and aids in meeting the following objective: O.PROTECTED\_COMMUNICATIONS.

#### FAU\_STG\_EXT.1 External Audit Trail Storage

This component ensures that the TSF is able to export audit records to an external audit server via a secure channel to protect the integrity and security of those records. This component traces back to and aids in meeting the following objective: O.SYSTEM\_MONITORING.

FAU\_STG\_EXT.3 Action in case of Loss of Audit Server Connectivity

This component ensures that the TSF is able to detect when the external audit server is not available and take an appropriate action. It also ensures the TSF is able to detect when its audit server is not available and take an appropriate action. This component traces back to and aids in meeting the following objectives: O.SYSTEM\_MONITORING and O.PROTECTED\_COMMUNICATIONS.

FCS\_HTTPS\_EXT.1 Explicit: HTTPS

This component ensures that the TSF will implement HTTPS properly to protect applicable network communication channel. This traces back to and aids in meeting the following objective: O.PROTECTED\_COMMUNICATIONS, and O.EAL.

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.

FCS\_IPSEC\_EXT.1 Explicit: IPSEC

This component ensures that the TSF will implement IPSEC properly to protect network communication channels with VPN clients and peers. This traces back to and aids in meeting the following objective: O.INTEGRITY.

FCS\_RBG\_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

This component ensures that the TSF will implement NIST- or FIPS-conformant Random Bit Generation in support of cryptographic protocol. This traces back to and aids in meeting the following objective: O.INTEGRITY, O.KEYCONF, and O.PROTECTED\_COMMUNICATIONS.

FCS\_SSH\_EXT.1 Explicit: SSH

This component ensures that the TSF will implement SSH properly to protect applicable network communication channels. This traces back to and aids in meeting the following objective: , O.PROTECTED\_COMMUNICATIONS, and O.EAL.

FCS\_TLS\_EXT.1 Explicit: TLS

This component ensures that the TSF will implement TLS properly to protect applicable network communication channels. This traces back to and aids in meeting the following objective: , O.PROTECTED\_COMMUNICATIONS, and O.EAL.

FIA\_PMG\_EXT.1 Password Management

This component ensures that the TSF will implement mechanisms allowing an administrator to constrain the construction of passwords to encourage more secure (or harder to guess) passwords. This traces back to and aids in meeting the following objective: O.TOE\_ADMINISTRATION.

FIA\_UAU\_EXT.5 Extended: Password-based Authentication Mechanism

This component ensures that the TSF implements a local authentication mechanism and can support additional authentication mechanisms. This traces back to and aids in meeting the following objective: O.TOE\_ADMINISTRATION.

FPT\_PTD\_EXT.1 Management of TSF Data (for reading of authentication data)

This component ensures that the TSF will prevent even administrators from readily accessing sensitive user and TSF data such as passwords. This traces back to and aids in meeting the following objectives: O.TOE\_ADMINISTRATION, and O.KEYCONF.

FPT\_PTD\_EXT.2 Management of TSF Data (for reading of all symmetric keys)

This component ensures that the TSF will prevent even administrators from readily accessing sensitive

---

user and TSF data such as cryptographic keys. This traces back to and aids in meeting the following objectives: O.PROTECTED\_COMMUNICATIONS, and O.KEYCONF.

**FPT\_TST\_EXT.1 TSF Testing**

This component ensures that the TSF will exercise self-tests during start-up to periodically ensure that the TOE security functions appear to be operating correctly. This traces back to and aids in meeting the following objective: O.TSF\_SELF\_TEST.

**FPT\_TUD\_EXT.1 Extended: Trusted Update**

This component ensures that the TSF will provide update functions and also the means for an administrator to initiate and verify updates before they are applied. This traces back to and aids in meeting the following objective: O.VERIFIABLE\_UPDATES.

## Glossary: Acronyms and Abbreviations

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

*Table 19 Acronyms or Abbreviations*

<b>Acronym Abbreviation</b>	<b>or</b>	<b>Definition</b>
AAA		Authentication, Authorization, and Accounting
ACE		Access Control Entry
ACL		Access Control List
AES		Advanced Encryption Standard
ASA		Adaptive Security Appliance
ASDM		Adaptive Security Device Manager
CA		Certificate Authority
CC		Common Criteria
DES		Data Encryption Standard
DH		Diffie Hellman (DH) Key Technique used to exchange private encryption keys.
DSA		Digital Signature Algorithm
DTLS		Datagram Transport Layer Security
EAL		Evaluation Assurance Level
ESP		Encapsulating Security Payload
FIPS		Federal Information Processing Standard
HTTPS		Hypertext Transfer Protocol Secure
IKE		Internet Key Exchange
IP		Internet Protocol
IPSec		IP tunneling protocol that manages encryption between multiple hosts using secure communication
LAN		Local Area Network
PP		Protection Profile
rDSA		RSA Digital Signature Algorithm

<b>Acronym Abbreviation</b>	<b>or</b>	<b>Definition</b>
RSA		Asymmetric cryptography algorithm developed by Rivest, Shamir, and Adleman
SA		Security Association
SAR		Security Assurance Requirements
SMB		Small and Medium-sized Business
SFP		Security Function Policy
SFR		Security Functional Requirements
SSH		Secure Shell
SSL		Secure Sockets Layer
ST		Security Target
TLS		Transport Layer Security
TOE		Target of Evaluation
TSAP		Transport Service Application Protocol
TSC		TOE Scope of Control
TSF		TOE Security Functions
TSP		TOE Security Policy
VLAN		Virtual LAN
VPN		Virtual Private Network

---

## 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.

[NDPP] “Security Requirements for Network Devices,” Version 1.0, 10 December 2010.

[CC\_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-001

[CC\_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated July 2009, version 3.1, Revision 3, CCMB--2009-07-002

[CC\_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-003

[CEM] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-004

## 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

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>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)  
© 2012 Cisco Systems, Inc. All rights reserved.