Cisco Adaptive Security Appliances

Security Target

Version 1.1

November, 2014

Americas Headquarters:

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

Table of Contents

List of Tables

List of Figures

List of Acronyms

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

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSM	Cisco Security Manager
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
Gbps	Gigabits per second
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IT	Information Technology
NDPP	Network Device Protection Profile
OS	Operating System
PoE	Power over Ethernet
POP3	Post Office Protocol
PP	Protection Profile
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SSHv2	Secure Shell (version 2)
SSM	Security Services Module
SSP	Security Services Processor
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
VLAN	Virtual Local Area Network

Acronyms / Abbreviations	Definition
WAN	Wide Area Network
WIC	WAN Interface Card

DOCUMENT INTRODUCTION

Prepared By:

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Adaptive Security Appliances (ASA). 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. Administrators of the TOE will be referred to as administrators, authorized administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- Rationale [Section 7]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 2.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Cisco Adaptive Security Appliances
ST Version	1.1
Publication Date	November, 2014
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Adaptive Security Appliances
TOE Hardware Models	ASA 5500 (5505, 5510, 5520, 5540, 5550, 5580-20-40), ASA 5500-X Series (5512-X, 5515-X, 5525-X, 5545-X, 5555-X), ASA 5585-X (5585-10, 5585-20, 5585-40, 5585-60), ASA Services Module (ASA-SM)
TOE Software Version	ASA 9.1(5.12) with ASDM 7.1(6)
ST Evaluation Status	PP Compliant
Keywords	Firewall, VPN, Router

1.2 TOE Overview

The Cisco Adaptive Security Appliances TOE is a purpose-built, firewall platform. The TOE includes the hardware models as defined in Table 2 in section 1.1.

1.2.1 TOE Product Type

The TOE consists of hardware and software that provide connectivity and security services onto a single, secure device.

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.

The Cisco ASA can operate in a number of modes: as a single standalone device, or in high-availability (HA) failover-pairs; with a single-context, or with multiple-contexts within each single/pair; as a transparent firewall when deployed in single-context, or with one or more contexts connected to two or many IP subnets when configured in router mode.

The Cisco ASA provides IPsec connection capabilities, but in the evaluated configuration those IPsec tunnels are only to be used to secure connectivity to or from the ASA, not to secure traffic through the ASA. All references within this ST to “VPN” connectivity refer to use of IPsec or TLS connections that are used to tunnel traffic that originates from or terminates at the ASA itself, such as for transmissions from the ASA to remote audit/syslog servers, or AAA servers, or for an additional layer of security for remote administration connections to the ASA, such as SSH or TLS connections tunneled in IPsec.

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

- TLS/HTTPS encrypted sessions.
- 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.

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 3: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSHv2 client installed that is used by the TOE administrator to support TOE administration through SSHv2 protected channels. Any SSHv2 client that supports SSHv2 may be used.
ASDM Management Platform	Yes	The ASDM 7.1(6) operates from any of the following operating systems: • Microsoft Windows XP (x86), including Service Pack 1, 2, and 3 • Windows Vista (x86 and x64), including Service Pack 1 and 2 • Windows 7 (x86 and x64) • Mac OS X 10.4 - 10.6 (x86 and x64) 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.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Connections to remote audit servers must be tunneled in IPsec or TLS.
RADIUS or TACACS+ AAA Server	No	This includes any IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators. Connections to remote AAA servers must be tunneled in IPsec.
Certification Authority	No	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
Remote tunnel endpoint	No	This includes any peer with which the TOE participates in tunneled communications. Remote tunnel endpoints may be any device or software client that supports IPsec or TLS tunneling. Both VPN clients and VPN gateways can be considered to be remote tunnel endpoints.
NTP Server	No	The TOE supports communications with an NTP server. Connections to remote NTP servers can optionally be tunneled in IPsec.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Adaptive Security Appliances Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following: ASA 5500 (5505, 5510, 5520, 5540, 5550, 5580-20-40), ASA 5500-X Series (5512-X, 5515-X, 5525-X, 5545-X, 5555-X), ASA 5585-X (5585-10, 5585-20, 5585-40, 5585-60), ASA Services Module (ASA-SM). The software is comprised of the Adaptive Security Appliance software image Release 9.1(5.12), with ASDM 7.1(6).

The Cisco Adaptive Security Appliances that comprise the TOE have common hardware characteristics. These differing characteristics affect only non-TSF relevant functionality (such as throughput, processing speed, number and type of network connections supported, number of concurrent connections supported, and amount of storage) and therefore support security equivalency of the routers in terms of hardware.

Figure 1: ASA Hardware Components

The ASA hardware components in the TOE have the following distinct characteristics:

- 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)
- 5512-X – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to twelve).
- 5515-X – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to twelve).
- 5525-X – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to fourteen).
- 5545-X – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to fourteen).
- 5555-X – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to fourteen).
- ASA-SM – Installs to Catalyst 6500 series switches including 6503-E, 6504-E, 6509-E, and 6513-E. All interfaces are virtual on the ASA-SM, allowing any port on the 6500 switch to operate as a firewall port and integrating firewall security inside the network infrastructure.

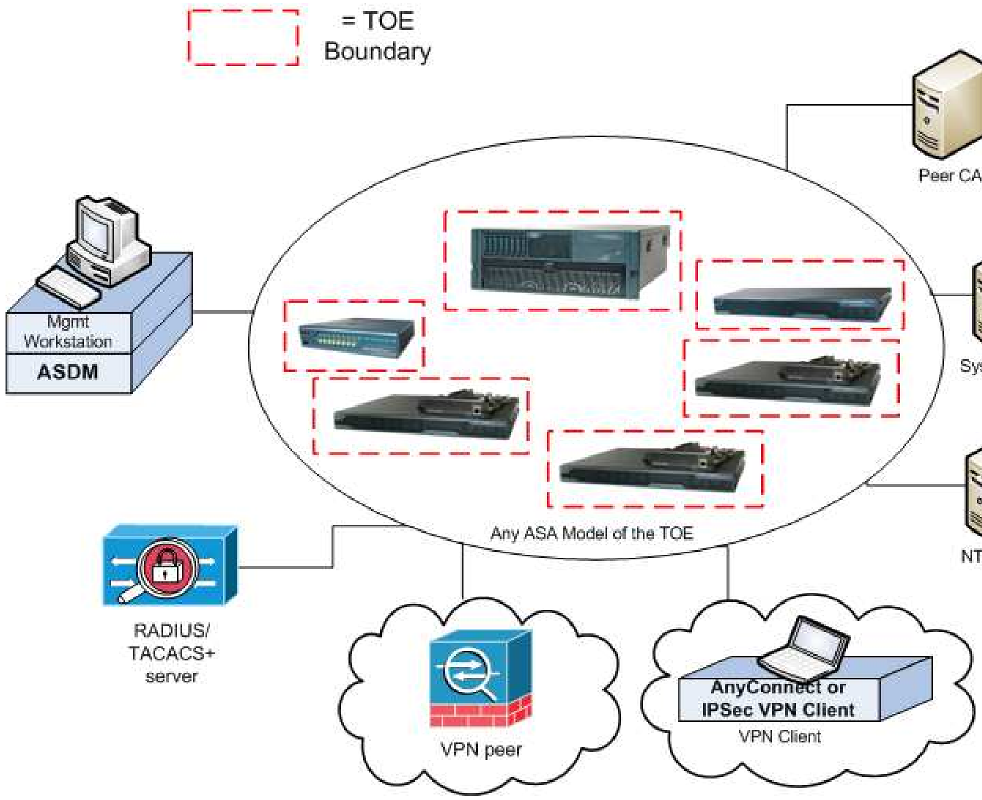
1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.5 below and includes the Cisco ASA software, which in turn includes the ASDM software. Each instantiation of the TOE has two or more network interfaces, and is able to filter IP traffic to and through those interfaces.

The TOE can optionally connect to an NTP server for clock updates. If the ASA is to be remotely administered, the management station must connect using SSHv2. When ASDM is used a remote workstation with a TLS-enabled browser must be available. A syslog server can also be used to store audit records, and the syslog server must support syslog over TLS or IPsec. The TOE is able to filter connections to/from these external using its IP traffic filtering, and can encrypt traffic where necessary using TLS, SSH, and/or IPsec.

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
- 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)

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution comprised of the components described in Table 4:

Table 4 Hardware Models and Specifications

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, and can support up to 25 VPNs.	ASA release 9.1(5.12)
ASA 5510	The Cisco ASA 5510 Adaptive Security	ASA release 9.1(5.12)

	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 250 VPNs.	
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 750 VPNs.	ASA release 9.1(5.12)
ASA 5540 	The Cisco ASA 5540 Adaptive Security Appliance provides high-performance firewall and VPN services and four Gigabit Ethernet interfaces and support for up to 2,500 VPNs.	ASA release 9.1(5.12)
ASA 5550 	The Cisco ASA 5540 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 5,000 VPNs.	ASA release 9.1(5.12)
ASA 5580-20 **ASA 5580-40** 	The Cisco ASA 5580 Adaptive Security Appliances provide six interface expansion card slots with support for up to 24 Gigabit Ethernet interfaces or up to 12 10Gigabit Ethernet interfaces or up to twenty-four 10/100/1000 Ethernet ports, and support for up to 10,000 VPNs.	ASA release 9.1(5.12)
ASA-5585-S10 **ASA-5585-S20** **ASA-5585-S40** **ASA-5585-S60** 	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 10,000 VPNs.	ASA release 9.1(5.12)
5512-X **5515-X** **5525-X** **5545-X** **5555-X** 	The Cisco ASA 5500-X Adaptive Security Appliance provides high-performance firewall and VPN services and 6-14 Gigabit Ethernet interfaces, and support for up to 5,000 VPNs.	ASA release 9.1(5.12)
ASA Services Module (ASA-SM)	The Cisco Catalyst 6500 Series ASA Services Module supports up to: 20 Gbps	ASA release 9.1(5.12)

	maximum firewall throughput (max); 16 Gbps of maximum firewall throughput (multi-protocol); 300,000 connections per second; 10 million concurrent connections; 250 security contexts.	
ASDM	Included on all ASA models with ASA 9.1(5.12).	Release 7.1(6)

1.6 Logical Scope of the TOE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptographic Support
3. Full Residual Information Protection
4. Identification and Authentication
5. Security Management
6. TOE Access
7. Trusted Path/Channels
8. Firewall

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

1.6.1 Security Audit

The Cisco Adaptive Security Appliances provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Adaptive Security Appliances generates an audit record for each auditable event. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are backed up over an encrypted channel to an external audit server.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of other Cisco ASA security functionality. The TOE provides cryptography in support of VPN connections using TLS and IPsec, and remote administrative management via SSHv2, and TLS/HTTPS.

1.6.3 Full Residual Information Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

1.6.4 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the authorized administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication.

The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI administrator interface. The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE optionally supports use of a RADIUS or TACACS+ AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE’s CLI.

1.6.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 or TLS/HTTPS session, or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users; all identification and authentication; all audit functionality of the TOE; all TOE cryptographic functionality; the timestamps maintained by the TOE; TOE configuration file storage and retrieval, and the information flow control policies enforced by the TOE including encryption/decryption of information flows for VPNs. The TOE supports an “authorized administrator” role, which equates to any account authenticated to an administrative interface (CLI or GUI, but not VPN), and possessing sufficient privileges to perform security-relevant administrative actions.

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. This is used to provide any information deemed necessary by the administrator. After a configurable period of inactivity, administrative sessions will be terminated, requiring administrators to re-authenticate.

1.6.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to authorized administrators. The TOE prevents reading of cryptographic keys and passwords.

Additionally Cisco ASA is not a general-purpose operating system and access to Cisco ASA memory space is restricted to only Cisco ASA functions.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source. Additionally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

1.6.7 TOE Access

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. This is used to provide any information deemed necessary by the administrator. After a configurable period of inactivity, administrative sessions will be terminated, requiring administrators to re-authenticate.

1.6.8 Trusted path/Channels

The TOE supports establishing trusted paths between itself and remote administrators using SSHv2 for CLI access, and TLS/HTTPS for GUI/ASDM access. The TOE supports use of TLS and/or IPsec for connections with remote syslog servers. The TOE can use IPsec to encrypt connections with remote authentication servers (e.g. RADIUS or TACACS+). The TOE can establish trusted paths of peer-to-peer VPN tunnels using IPsec, and VPN client tunnels using IPsec or TLS.

1.6.9 Firewall

The TOE provides stateful traffic firewall functionality including IP address-based filtering (for IPv4 and IPv6) to address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance. Address filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on source and/or destination IP addresses. Port filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (service). Stateful packet inspection is used to aid in the performance of packet flow through the TOE and to ensure that only packets are only forwarded when they're part of a properly established session. The TOE supports protocols that can spawn additional sessions in accordance with the protocol RFCs where a new connection will be implicitly permitted when properly initiated by an explicitly permitted session. The File Transfer Protocol is an example of such a protocol, where a data connection is created as needed in response to an explicitly allowed command connection. System monitoring functionality includes the ability to generate audit messages for any explicitly defined (permitted or denied) traffic flow. TOE administrators have the ability to configure permitted and denied traffic flows, including adjusting the sequence in which flow control rules will be applied, and to apply rules to any network interface of the TOE.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 5: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Secure Policy Manager is excluded from the evaluated configuration	Use of Security Policy Manager is beyond the scope of this Common Criteria evaluation.
Filtering of non-IP traffic provided by the EtherType option when configuring information flow policies is excluded from the evaluated configuration	Use of non-IP traffic filtering is beyond the scope of this Common Criteria evaluation.
Smart Call Home. The Smart Call Home feature provides personalized, e-mail-based and web-based notification to customers about critical events involving their individual systems.	Use of Smart Call Home is beyond the scope of this Common Criteria evaluation.
Use of Secure Copy (outbound client)	Use of Secure Copy is beyond the scope of this Common Criteria evaluation.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) and Traffic Filter Firewall Extended Package (TFFWEP).

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012. For a listing of Assurance Requirements claimed see section 5.6.

The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 6 below:

Table 6: Protection Profiles

Protection Profile	Version	Date
U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) and Traffic Filter Firewall Extended Package (TFFWEP) (NDPP)	1.1	June 8, 2012
NDPP and TFFWEP (TFFWEP)	1.0	December 19, 2011

2.2.1 Protection Profile Additions

The following requirement was modified:

- FMT_SMF.1 – A refinement was added "***Ability to configure the firewall rules.***" This refinement was added in order to be compliant with the NDPP and TFFWEP section 4.2.3.

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profiles:

- U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) and Traffic Filter Firewall Extended Package (TFFWEP)

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) and Traffic Filter Firewall Extended Package (TFFWEP) for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in the U.S. Government Protection Profile for Security Requirements for Network

Devices for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) and Traffic Filter Firewall Extended Package (TFFWEP) for which conformance is claimed verbatim and several additional Security Functional Requirements are also included. All concepts covered the Protection Profile's Statement of Security Requirements are included in the Security Target. Additionally, the Security Assurance Requirements included in the Security Target are identical to the Security Assurance Requirements included in section 4.3 of the NDPP.

3 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. Organizational Security Policies (OSPs) are identified as P.osp with "osp" specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's 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 7 TOE Assumptions

Assumption	Assumption Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
Reproduced from the TFFWEP	
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

3.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 8 Threats

Threat	Threat Definition
Reproduced from the NDPP	
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.

Threat	Threat Definition
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.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.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.
Reproduced from the TFFWEP	
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T. NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies.
T.NETWORK_DOS	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network.

3.3 Organizational Security Policies

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

Table 9 Organizational Security Policies

Policy Name	Policy Definition
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.

4 SECURITY OBJECTIVES

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

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

4.1 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 10 Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
Reproduced from the NDPP	
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
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.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
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.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
Reproduced from the TFFWEP	
O.ADDRESS_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination addresses.
O.PORT_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination

TOE Objective	TOE Security Objective Definition
	transport layer ports.
O.STATEFUL_INSPECTION	The TOE will determine if a network packet belongs to an allowed established connection before applying the ruleset.
O.RELATED_CONNECTION_FILTERING	For specific protocols, the TOE will dynamically permit a network packet flow in response to a connection permitted by the ruleset.

4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 11 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
Reproduced from the NDPP	
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
Reproduced from the TFFWEP	
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012* and all international interpretations.

5.1 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:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated with **bold** text;
- Selection: Indicated with <u>underlined</u> text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the NDPP itself, the formatting used in the NDPP has been retained.

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs. Formatting conventions outside of operations and iterations matches the formatting specified within the NDPP.

5.2 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 12 Security Functional Requirements

Class Name	**Component Identification**	**Component Name**
Security Functional Requirements Drawn from NDPP		
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic Operation (for keyed-hash message authentication)
	FCS_HTTPS_EXT.1	Explicit: HTTPS
	FCS_IPSEC_EXT.1	Explicit: IPSEC
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit

Class Name	Component Identification	Component Name
		Generation)
	FCS_TLS_EXT.1	Explicit: TLS
	FCS_SSH_EXT.1	Explicit: SSH
FDP: User data protection	FDP_RIP.2	Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
FMT: Security management	FMT_MTD.1	Management of TSF Data (for general TSF data)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_STM.1	Reliable Time Stamps
	FPT_TUD_EXT.1	Extended: Trusted Update
	FPT_TST_EXT.1	TSF Testing
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Trusted Channel
	FTP_TRP.1	Trusted Path
Reproduced from the TFFWEP		
FFW: Stateful Traffic Filtering	FFW_RUL_EXT.1	Stateful Traffic Filtering

5.3 SFRs Drawn from NDPP

5.3.1 Security audit (FAU)

5.3.1.1 FAU_GEN.1 Audit data generation

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions;
d) [Specifically defined auditable events listed in Table 13].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of* Table 13].

Table 13 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FCS_CKM.1	None.	
FCS_CKM_EXT.4	None.	
FCS_COP.1(1)	None.	
FCS_COP.1(2)	None.	
FCS_COP.1(3)	None.	
FCS_COP.1(4)	None.	
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session. Establishment/Termination of an HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Establishment/Termination of an IPsec SA.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	None.	
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.
FCS_TLS_EXT.1	Failure to establish an TLS session Establishment/Termination of an TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None.	
FIA_PMG_EXT.1	None.	
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.2	None.	
FPT_SKP_EXT.1	None.	
FPT_APW_EXT.1	None.	
FPT_ITT.1	None.	None.
FPT_STM.1	Changes to the time.	The old and new values for the time. 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”.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session	No additional information.

SFR	Auditable Event	Additional Audit Record Contents
	by the session locking mechanism.	
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_TAB.1	None.	
FTP_ITC.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_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.
FFW_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets

5.3.1.2 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.

5.3.1.3 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] using a trusted channel implementing the [IPsec, TLS] protocol.

5.3.2 Cryptographic Support (FCS)

5.3.2.1 FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1 Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance with

[• NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes]

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

5.3.2.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.3.2.3 FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1(1) Refinement: The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES operating in* [***CBC, GCM, and GMAC modes,***]] and cryptographic key sizes 128-bits, 256-bits, and [192 bits] that meets the following:

- FIPS PUB 197, "Advanced Encryption Standard (AES)"
- [NIST SP 800-38A]

5.3.2.4 FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2) Refinement: The TSF shall perform cryptographic signature services in accordance with a [

RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater]

that meets the following:[

- FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard"]

5.3.2.5 FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1(3) Refinement: The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

5.3.2.6 FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1(4) Refinement: The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm HMAC-[SHA-1, SHA-256, SHA-384, SHA-512], key size [*160, 256, 512*], and message digest sizes [160, 256, 384, 512] bits that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."*

5.3.2.7 FCS_HTTPS_EXT.1 Explicit: 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.

5.3.2.8 FCS_IPSEC_EXT.1 Explicit: IPSEC

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec protocol ESP 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, RFC 4109, and [no other RFCs for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [no other RFCs for hash functions]].

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), 21 (521-bit Random ECP)*.

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: ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "?", space , tilde~, hyphen-, underscore _, plus+, equal=, curly-brackets{}, square-brackets[], vertical-bar(pipe)|, forward-slash/, back-slash\, colon:, semi-colon;, double-quote", single-quote', angle-brackets<>, comma,, and period.];*
2. Pre-shared keys of 22 characters and [*up to 128 characters*].

5.3.2.9 FCS_RBG_EXT.1 Extended: 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 AES (for single-core platforms: 5505, 5510, 5520, 5540, and 5550), and NIST Special Publication 800-90 using Hash_DRBG with SHA-512 (for multi-core platforms: 5512, 5515, 5525, 5545, 5555, 5580, 5585, and the ASA SM)] seeded by an entropy source that accumulated entropy from [a software-based noise source; a TSF-hardware-based noise source].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [128 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

5.3.2.10 FCS_SSH_EXT.1 Explicit: 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 protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*65,535 bytes*] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 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.1.5 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.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [*hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96*].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.3.2.11 FCS_TLS_EXT.1 Explicit: TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.0 (RFC 2246)] 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].

5.3.3 User data protection (FDP)

5.3.3.1 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.

5.3.4 Identification and authentication (FIA)

5.3.4.1 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 the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “ ” ‘ ` *(double or single quote/apostrophe), + (plus), - (minus), = (equal), , (comma), . (period), / (forward-slash), \ (back-slash), | (vertical-bar or pipe), : (colon), ; (semi-colon), < > (less-than, greater-than inequality signs), [ ] (square-brackets), { } (braces or curly-brackets),? (question-mark), ^ (caret), _ (underscore), and ~ (tilde)*];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

5.3.4.2 FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [*Download ASDM*]

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated action on behalf of that administrative user.

5.3.4.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [*support for RADIUS and TACACS+*] to perform administrative user authentication.

5.3.4.4 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress at the local console.

5.3.5 Security management (FMT)

5.3.5.1 FMT_MTD.1 Management of TSF Data (for general TSF data)

FMT_MTD.1.1 The TSF shall restrict the ability to *manage* the *TSF data* to the *Security Administrators*.

5.3.5.2 FMT_SMF.1 Specification of Management Functions

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

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using [published hash] capability prior to installing those updates;
- [Ability to configure the cryptographic functionality]

5.3.5.3 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- Authorized Administrator.

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;

are satisfied.

5.3.6 Protection of the TSF (FPT)

5.3.6.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 Refinement: The TSF shall protect TSF data from *disclosure* ***and detect its modification*** when it is transmitted between separate parts of the TOE **through the use** [**of: TLS, TLS/HTTPS**].

5.3.6.2 FPT_SKP_EXT.1 Extended: Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.3.6.3 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

5.3.6.4 FPT_STM.1 Reliable time stamps

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

5.3.6.5 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.

5.3.6.6 FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to 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.

5.3.7 TOE Access (FTA)

5.3.7.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [

- terminate the session]

after a Security Administrator-specified time period of inactivity.

5.3.7.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 Refinement: The TSF shall terminate **a remote** interactive session after a [*Security Administrator-configurable time interval of session inactivity*].

5.3.7.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.3.7.4 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Refinement: Before establishing **an administrative user** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

5.3.1 Trusted Path/Channels (FTP)

5.3.1.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall use [IPsec, SSH, TLS, TLS/HTTPS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [authentication server, *TLS server; intrusion prevention system (IPS)*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit *the TSF, or the **authorized IT entities*** to initiate communication via the trusted channel.

FTP_ ITC.1.3 The TSF shall initiate communication via the trusted channel for [

- *Audit server: transmit audit data via syslog over TLS or syslog over IPsec;*
- *Authentication server: authentication of TOE administrators using AAA servers including RADIUS over IPsec and TACACS+ over IPsec;*
- *TLS server: copy (upload or download) software images or configuration files*].

5.3.1.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 Refinement: The TSF shall **use** [**IPsec, SSH, TLS, TLS/HTTPS**] provide a **trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *disclosure and detection of modification of the communicated data*.

FTP_TRP.1.2 Refinement: The TSF shall permit **remote administrators** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

5.4 SFRs from the TFFWEP PP

5.4.1 Stateful traffic filtering (FFW)

5.4.1.1 FFW_RUL_EXT.1 Stateful Traffic Filtering

FFW_RUL_EXT.1.1 The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE.

FFW_RUL_EXT.1.2 The TSF shall process the following network traffic protocols:

- Internet Control Message Protocol version 4 (ICMPv4)
- Internet Control Message Protocol version 6 (ICMPv6)
- Internet Protocol (IPv4)

- Internet Protocol version 6 (IPv6)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

and be capable of inspecting network packet header fields defined by the following RFCs to the extent mandated in the other elements of this SFR

- RFC 792 (ICMPv4)
- RFC 4443 (ICMPv6)
- RFC 791 (IPv4)
- RFC 2460 (IPv6)
- RFC 793 (TCP)
- RFC 768 (UDP).

FFW_RUL_EXT.1.3 The TSF shall allow the definition of Stateful Traffic Filtering rules using the following network protocol fields:

- ICMPv4
  - Type
  - Code
- ICMPv6
  - Type
  - Code
- IPv4
  - Source address
  - Destination Address
  - Transport Layer Protocol
- IPv6
  - Source address
  - Destination Address
  - Transport Layer Protocol
- TCP
  - Source Port
  - Destination Port
- UDP
  - Source Port
  - Destination Port

FFW_RUL_EXT.1.4 The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules: permit, deny, and log.

FFW_RUL_EXT.1.5 The TSF shall allow the Stateful Traffic Filtering rules to be assigned to each distinct network interface.

FFW_RUL_EXT.1.6 The TSF shall:

a) accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols: TCP, UDP, [ICMP] based on the following network packet attributes:

1. TCP: source and destination addresses, source and destination ports, sequence number, Flags;

2. UDP: source and destination addresses, source and destination ports;

3. [ICMP: source and destination addresses, [type, code]].

b) Remove existing traffic flows from the set of established traffic flows based on the following: [session inactivity timeout, completion of the expected information flow].

FFW_RUL_EXT.1.7 The TSF shall be able to process the following network protocols:

1. FTP,

2. [no other protocols],

to dynamically define rules or establish sessions allowing network traffic of the following types:

- FTP: TCP data sessions in accordance with the FTP protocol as specified in RFC 959,
- [*none]*

FFW_RUL_EXT.1.8 The TSF shall enforce the following default Stateful Traffic Filtering rules on all network traffic:

1. The TSF shall reject and be capable of logging packets which are invalid fragments;
2. The TSF shall reject and be capable of logging fragmented IP packets which cannot be re-assembled completely;
3. The TSF shall reject and be capable of logging network packets where the source address of the network packet is equal to the address of the network interface where the network packet was received;
4. The TSF shall reject and be capable of logging network packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received;
5. The TSF shall reject and be capable of logging network packets where the source address of the network packet is defined as being on a broadcast network;
6. The TSF shall reject and be capable of logging network packets where the source address of the network packet is defined as being on a multicast network;
7. The TSF shall reject and be capable of logging network packets where the source address of the network packet is defined as being a loopback address;
8. The TSF shall reject and be capable of logging network packets where the source address of the network packet is a multicast;
9. The TSF shall reject and be capable of logging network packets where the source or destination address of the network packet is a link-local address;
10. The TSF shall reject and be capable of logging network packets where the source or destination address of the network packet is defined as being an address "reserved for future use" as specified in RFC 5735 for IPv4;
11. The TSF shall reject and be capable of logging network packets where the source or destination address of the network packet is defined as an "unspecified

address" or an address "reserved for future definition and use" as specified in RFC 3513 for IPv6;

12. The TSF shall reject and be capable of logging network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified; and
13. Other traffic dropped by default and able to be logged:
    i. Slowpath Security Checks – The TSF shall reject and be capable of logging the detection of the following network packets:
        1. In routed mode when the ASA receives a through-the-box:
            a. L2 broadcast packet (MAC address FF:FF:FF:FF:FF:FF)
            b. IPv4 packet with destination IP address equal to 0.0.0.0
            c. IPv4 packet with source IP address equal to 0.0.0.0
        2. In routed or transparent mode when the ASA receives a through-the-box IPv4 packet with any of:
            a. first octet of the source IP address equal to zero
            b. network part of the source IP address equal to all 0's
            c. network part of the source IP address equal to all 1's
            d. source IP address host part equal to all 0's or all 1's
            e. source IP address and destination IP address are the same ("land.c" attack)
        3. IPv6 through-the-box packet with identical source and destination address.

    ii. LAND Attack: The TSF shall reject and be capable of logging network packets with the IP source address equal to the IP destination, and the destination port equal to the source port.

    iii. ICMP Error Inspect and ICMPv6 Error Inspect - The TSF shall reject and be capable of logging ICMP error packets when the ICMP error messages are not related to any session already established in the ASA.

    iv. ICMPv6 condition - The TSF shall reject and be capable of logging network packets when the appliance is not able to find any established connection related to the frame embedded in the ICMPv6 error message.

    v. ICMP Inspect bad icmp code - The TSF shall reject and be capable of logging network packets when an ICMP echo request/reply packet was received with a malformed code(non-zero).

FFW_RUL_EXT.1.9 When FFW_RUL_EXT.1.6 or FFW_RUL_EXT.1.7 do not apply, the TSF shall process the applicable Stateful Traffic Filtering rules (as determined in accordance with FFW_RUL_EXT.1.5) in the following order: administrator-defined.

FFW_RUL_EXT.1.10 When FFW_RUL_EXT.1.6 or FFW_RUL_EXT.1.7 do not apply, the TSF shall deny packet flow if a matching rule is not identified.

5.5 TOE SFR Dependencies Rationale for SFRs Found in NDPP

The NDPPv1.1 contains all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PP itself has been approved.

5.6 Security Assurance Requirements

5.6.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDPP which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 14: Assurance Measures

Assurance Class	Components	Components Description
DEVELOPMENT	ADV_FSP.1	Basic Functional Specification
GUIDANCE DOCUMENTS	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
LIFE CYCLE SUPPORT	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
TESTS	ATE_IND.1	Independent testing - conformance
VULNERABILITY ASSESSMENT	AVA_VAN.1	Vulnerability analysis

5.6.2 Security Assurance Requirements Rationale

This Security Target claims conformance to the NDPP, which essentially is an EAL1+ conformance claim. This target was chosen to ensure that the TOE has a low to 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. The ST also claims conformance to the TFFWEP, which includes refinements to assurance measures for the SFRs defined in the TFFWEP, including augmenting the vulnerability analysis (AVA_VAN.1) with specific vulnerability testing.

5.7 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 15: Assurance Measures

Component	How requirement will be met

Component	How requirement will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ALC_CMS.1	
ATE_IND.1	Cisco provides the TOE for testing.
AVA_VAN.1	Cisco provides the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

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

Table 16: How TOE SFRs Are Satisfied

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Satisfied</th></tr>
<tr><td colspan="2"><b>Security Functional Requirements Drawn from NDPP</b></td></tr>
<tr><td>FAU_GEN.1</td><td>Shutdown and start-up of the audit functions are logged by events for reloading the ASA, and the events when the ASA comes back up. When audit is enabled, it is on whenever the TOE is on. Also, if logging is ever disabled, it is displayed in the ASDM Real-Time Log Viewer as a syslog disconnection and then a reconnection once it is re-established followed by an event that shows that the "logging enable" command was executed. See the table within this cell for other required events and rationale.
ASA generates events in the following format, with fields for date and time, type of event (the ASA-x-xxxxxx identifier code), subject identities, and outcome of the event:
Nov 21 2012 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.
Network interfaces have bandwidth limitations, and other traffic flow limitations that are configurable. When an interface has exceeded a limit for processing traffic, traffic will be dropped, and audit messages can be generated, such as:
Nov 21 2012 20:39:21: %ASA-3-201011: Connection limit exceeded <i>cnt</i>/<i>limit</i> for <i>dir</i> packet from <i>sip</i>/<i>sport</i> to <i>dip</i>/<i>dport</i> on interface <i>if_name</i>.
Nov 21 2012 20:39:21: %ASA-3-202011: Connection limit exceeded <i>econns/limit</i> for <i>dir</i> packet from <i>source_address/source_port</i> to <i>dest_address/dest_port</i> on interface <i>interface_name</i>
The following events are auditable by the TOE:
<table>
<tr><th>Auditable Event</th><th>Rationale</th></tr>
<tr><td>Modifications to the group of users that are part of the authorized administrator role.</td><td>All changes to the configuration (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>All use of the user identification mechanism.</td><td>Events will be generated for attempted identification/ authentication, and the username attempting to authenticate will be recorded in the event.</td></tr>
<tr><td>Any use of the authentication mechanism.</td><td>Events will be generated for attempted identification/ authentication, and the username attempting to authenticate will be recorded in the event along with the origin or source of the attempt.</td></tr>
</table>
</td></tr>
</table>

TOE SFRs	How the SFR is Satisfied	
	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.
	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.
	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets

TOE SFRs	How the SFR is Satisfied
FAU_GEN.2	The ASA ensures each action performed by the administrator at the CLI or via ASDM is logged with the administrator's identity and as a result events are traceable to a specific user.
FAU_STG_EXT.1	The ASA can be configured export syslog records to an administrator-specified, external syslog server. The ASA can be configured to encrypt the communications with an external syslog server using TLS or IPsec. If using syslog over TLS, or TCP syslog through an IPsec tunnel, the ASA can be configured to 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(s). The ASA will buffer syslog messages locally, but the local buffer will be cleared when the ASA is rebooted. The default size of the buffer is 4KB, and can be increased to 16KB. When the local buffer is full, the oldest message will be overwritten with new messages.
FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1) through (4), and FCS_RBG_EXT.1	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. Key generation for asymmetric keys on all models of the ASA implements RSA-based key establishment schemes as specified in NIST SP 800-56B "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" with key sizes greater than 112 bit key strength. The shall(not) and should(not) statements from NIST SP 800-56B that are implemented (or not) by the ASA are itemized in section 8.3. The ASA meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs). Additional key zeroization detail is provided in section 8.2. An example of manually triggering zeroization is: existing RSA keys will be zeroized when new RSA keys are generated, and zeroization of RSA keys can be triggered manually through use of the command: asa(config)#**crypto key zeroize rsa** [label key-pair-label] [default] [noconfirm] The ASA supports AES-CBC, AES-GCM, and AES-GMAC, each with 128, 192, or 256-bit (as described in NIST SP 800-38A). The ASA uses a FIPS-validated implementation of AES with 128, 192, and 256 bit keys. Configuring the ASA software in or out of FIPS mode does not modify the ASA's use of the FIPS-validated AES. • ASA 9.1(5) software: FIPS certifications #2483 & #2482 • CN505 (ASA-5505) FIPS #2049 • CN1010 (ASA-5510, 5520, 5540, 5550) FIPS #105 • CN1610 (ASA-5512-X, 5515-X, 5525-X) FIPS #2472 • CN1520 (ASA-5580-20, 5580-40) FIPS #1407 & #2480 • CN1620 (ASA-5545-X, 5555-X, 5585-X SSP10/20/40/60) FIPS #2050 & #2444 The ASA provides cryptographic signature services using RSA with key sizes (modulus) of 2048 bits. The key size is configurable down to 1024, but only 2048 is

TOE SFRs	How the SFR is Satisfied
	permitted in the evaluated configuration. • ASA 9.1(2) software: FIPS certifications #1272 & #1271 • CN505 (ASA-5505) FIPS #261 • CN1010 (ASA-5510, 5520, 5540, 5550) FIPS #106 • CN1610 (ASA-5512-X, 5515-X, 5525-X) FIPS #1260 • CN1520 (ASA-5580-20, 5580-40) FIPS #1269 • CN1620 (ASA-5545-X, 5555-X, 5585-X SSP10/20/40/60) FIPS #1066 The ASA provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512, and keyed-hash message authentication using HMAC-SHA-1 (160-bit), HMAC-SHA-256 (256-bit), HMAC-SHA-384 (384-bit), and HMAC-SHA-512 (512-bit). • ASA 9.1(2) software: FIPS certifications #2101 & #2482 • CN505 (ASA-5505) FIPS #630 • CN1010 (ASA-5510, 5520, 5540, 5550) FIPS #196 • CN1610 (ASA-5512-X, 5515-X, 5525-X) FIPS #2091 • CN1520 (ASA-5580-20, 5580-40) FIPS #1407 & #1793 • CN1620 (ASA-5545-X, 5555-X, 5585-X SSP10/20/40/60) FIPS #1794 Random number generation in the TOE uses different methods depending on the underlying hardware. The ASA single-core platforms (5505, 5510, 5520, 5540, and 5550) use an X9.31 PRNG with AES-256. The ASA multi-core platforms (5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5580-X, 5585-X, and the ASASM) use a NIST SP800-90 Hash DRBG with SHA-512. The following Cavium NITROX (CN) security processors are used to generate entropy for random number generation: • ASA 9.1(2) software: FIPS certifications #1201 & #341 • CN505 (ASA-5505) FIPS #1210 • CN1010 (ASA-5510, 5520, 5540, 5550) FIPS #1210 • CN1610 (ASA-5512-X, 5515-X, 5525-X) FIPS #336 • CN1520 (ASA-5580-20, 5580-40) FIPS #1407 & #339 • CN1620 (ASA-5545-X, 5555-X, 5585-X SSP10/20/40/60) FIPS #332 Note: FIPS Change Letter was approved updating the FIPS 140-2 Level 2 full evaluation [Cert #2176] from software v9.1.2 to v9.1.5. The references to certificate algorithm numbers in the TSS remain unchanged. Refer to links to the FIPS cert page and the FIPS Security Policy that explicitly mention ASA 9.1.5. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2176 http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2176.pdf
FCS_HTTPS_EXT.1, and FCS_TLS_EXT.1	The ASA implements HTTS over TLS to support remote administration using ASDM. A remote administrator can connect over TLS to the ASA with their web browser and load the ASDM software from the ASDM. ASDM communicates with the ASA using HTTPS over TLS. The ASA will support TLS v1.0 connections with any of the following ciphersuites: • TLS_RSA_WITH_AES_128_CBC_SHA

TOE SFRs	How the SFR is Satisfied
	• TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA
FCS_IPSEC_EXT.1	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 IKEv2, as specified for FCS_IKE_EXT.1, to establish security associations. NAT traversal is supported in IKEv2 by default. 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. Administrators can require use of main mode by configuring the mode for each IPsec tunnel, as in the following examples: **asa(config)#crypto map** *map-name seq-num* **set ikev2 phase1-mode main** **asa(config)#crypto map** *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*} In the certified configuration, use of "confidentiality only" (i.e. using ESP without authentication) for IPsec connections is prohibited. The ASA allows the administrator to define the IPsec proposal for any IPsec connection to use specific encryption methods and authentication methods as in the following examples: asa(config)#**crypto ipsec ikev2 ipsec-proposal** *proposal tag proposal_name* asa(config-ipsec-proposal)#**protocol esp encryption** {aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256} asa(config-ipsec-proposal)#**protocol esp integrity** {sha-1 | sha-256 | sha-384 | sha-512 | null} **Note:** When AES-GCM, or AES-GMAC are used for encryption, the ESP integrity selection will be "null" because GCM and GMAC provide integrity. 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), 20 (384-bit Random EC), and 21 (*521-bit Random ECP*), and use the rDSA algorithm for Peer Authentication. The following command is used to specify the DH Group used for SAs: asa(config)#**crypto ikev2 policy** *priority policy_index* asa(config-ikev2-policy)#**group** {14 | 19 | 20 | 24} The ASA can be configured to authenticate IPsec connections using RSA signatures. When using RSA signatures for authentication, the ASA and its peer must be configured to obtain certificates from the same certification authority (CA). To configure an IKEv2 connection to use an RSA signature: asa(config)#**tunnel-group** *name* **ipsec-attributes** asa(config-tunnel-ipsec)#**ikev2** {local-authentication | remote-authentication} **certificate** *trustpoint* 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. The pre-shared keys can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "?", space " ", tilde~, hyphen-, underscore_, plus+, equal=, curly-brackets{}, square-brackets[], vertical-bar(pipe)|, forward-slash/, back-slash\, colon:, semi-colon;, double-quote", single-

TOE SFRs	How the SFR is Satisfied
	quote‘, angle-brackets<>, comma,, and period., and can be 1-128 characters in length. When using pre-shared keys for authentication, the IPsec endpoints must both be configured to use the same key. To configure an IKEv2 connection to use a pre-shared key: asa(config)#**tunnel-group** *name* **ipsec-attributes** asa(config-tunnel-ipsec)#**ikev2** {local-authentication | remote-authentication} **pre-shared-key** *key-value*
FCS_SSH_EXT.1	The TOE implements SSHv2 (telnet is disabled in the evaluated configuration). SSHv2 sessions are limited to a configurable session timeout period of 120 seconds, a maximum number of failed authentication attempts limited to 3, and will be rekeyed upon request from the SSH client. SSH connections will be dropped if the TOE receives a packet larger than 65,535 bytes. The ASA’s implementation of SSHv2 supports: • public key algorithm RSA for signing and verification; • password-based authentication for administrative users; • encryption algorithms, AES-CBC-128, AES-CBC-256 to ensure confidentiality of the session; • hashing algorithms hmac-sha1, hmac-sha1-96, hmac-md5, and hmac-md5-96 to ensure the integrity of the session. • requiring use of DH group 14 by using the following command when enabling SSHv2 on an interface: asa(config)#**ssh key-exchange dh-group14** {*ip_address mask* | *ipv6_address/prefix*} *interface*
FDP_RIP.2	The TOE ensures that packets transmitted from the TOE do not contain residual information from previous packets. Packets that are not the required length use zeros for padding. Residual data is never transmitted from the TOE. Packet handling within memory buffers ensures new packets cannot contain portions of previous packets. This applies to both data plane traffic and administrative session traffic.
FIA_PMG_EXT.1	The TOE 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 as listed in the SFR. Minimum password length is settable by the Authorized Administrator, and support passwords of 8 to 128 characters. Password composition rules specifying the types and number of required characters that comprise the password are settable by the Authorized Administrator. Passwords can be configured with a maximum lifetime, configurable by the Authorized Administrator. New passwords can be required to contain a minimum of 4 character changes from the previous password.
FIA_UIA_EXT.1	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through the TOE’s CLI (SSH or console), and through the GUI

TOE SFRs	How the SFR is Satisfied
	(ASDM). The TOE mediates all administrative actions through the CLI and GUI. Once a potential administrative user attempts to access an administrative interface either locally or remotely, the TOE prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated.
FIA_UAU_EXT.2	The TOE provides a local password based authentication mechanism as well as RADIUS and TACACS+ authentication. The administrator authentication policies include authentication to the local user database or redirection to a remote authentication server. Interfaces can be configured to try one or more remote authentication servers, and then fail back to the local user database if the remote authentication servers are inaccessible. The TOE can invoke an external authentication server to provide a single-use authentication mechanism by forwarding the authentication requests to the external authentication server (when configured by the TOE to provide single-use authentication). The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via SSHv2 or TLS. At initial login in the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and password is correct) or indicates that the login was unsuccessful. The TOE does not provide indication of whether the username or password was the reason for an authentication failure.
FIA_UAU.7	When a user enters their password at the local console, the ISR displays only '*' characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.
FMT_MTD.1	The TOE provides the ability for authorized administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds. Each of the predefined and administratively configured privilege level has delete set of permissions that will grant them access to the TOE data, though with some privilege levels, the access is limited. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged levels. For the purposes of this evaluation, the privileged level is equivalent to full administrative access to the CLI or GUI, and equivalent to privilege level 15. The term "authorized administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action.
FMT_SMF.1	The ASA is configured to restrict the ability to enter privileged configuration mode to level 15 users (the authorized administrator) once aaa authorizations has been enabled. Privileged configuration (EXEC) mode is where the commands are

TOE SFRs	How the SFR is Satisfied
	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. 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 commends. 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). 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 configurations are done through the ‘Configuration’ page.
FMT_SMR.2	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 > Device Management > Users/AAA > User Accounts’ page. 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. 'aaa authentication ssh console LOCAL' can be used to set the ASA to authenticate SSH users against the local database. 'aaa authorization exec' can be used to require re-authentication of users before they can get to EXEC mode. 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”. When command authorization has been enabled the default sets of privileges take effect at certain levels, and the levels become customizable. • When “aaa authorization command LOCAL” has NOT been applied to the config: o 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

TOE SFRs	How the SFR is Satisfied
	effectively at level 2 or higher. o 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). o Usernames with privilege levels 2-14 can login to ASDM, and have full read-write access. o Privilege levels cannot be customized. • When "aaa authorization command LOCAL" has been applied to the config: o 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. o Privilege levels (including levels 3 and 5) can be customized from the default to add/remove specific privileges. 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".
FPT_ITT.1	Connection between ASA components occurs in three situations: when ASDM is used for remote administration; when clustering is configured; and when failover is configured. The ASDM-to-ASA connections (for remote administration) will use TLS/HTTPS (optionally encapsulated in TLS if connecting from Cisco AnyConnect Secure Mobility Client). Clustering is a feature used for load-balancing VPN connections, but use of site-to-site VPNs (for any purpose other than securing traffic flows that originate from or terminate to the ASA itself) is out of scope for this evaluated configuration, so will not be used in the TOE. In the certified configuration, IPsec tunnels are not approved for the purpose of tunneling traffic between hosts across the ASA. Failover connections can be made through use of a proprietary serial cable, or via network connection. The serial cable connection can be used in the evaluated configuration of the TOE as it is not a network-based connection, but network-based failover must remain disabled in the evaluated configuration because the proprietary AES-based encryption used for that link is not conformant to any of the encryption protocols allowed by the NDPP.
FPT_SKP_EXT.1	The ASA stores all private keys in a secure directory (an 'opaque' virtual filesystem in RAM called "system:") that is not readily accessible to administrators. All pre-shared and symmetric keys are stored in encrypted form, or are masked when showing the configuration via administrative interfaces (CLI or GUI).
FPT_APW_EXT.1	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.
FPT_STM.1	The ASA provides a source of date and time information for the firewall, used in audit timestamps, in validating service requests, and for tracking time-based actions related to session management including timeouts for inactive administrative sessions (FTA_SSL_EXT.*), and renegotiating SAs for IPsec tunnels (FCS_IPSEC_EXT.1). This function can only be accessed from within the

TOE SFRs	How the SFR is Satisfied
	configuration exec mode via the privileged mode of operation of the firewall. The clock function is reliant on the system clock provided by the underlying hardware. This functionality can be set at the CLI using the 'clock' commands or in ASDM through the 'Configuration > Device Setup > System Time' page. The TOE can optionally be set to receive time from an NTP server. All ASA models in the TOE contain a hardware-based real-time-clock (RTC) with battery-backup that maintains time in the event of power loss or reboot. The clock's date and time can be adjusted by authorized administrators, and authorized administrators can configure the ASA to use clock updates from NTP servers. The ASA supports use of NTP version 3, which supports use of hashing to authenticate clock updates, but use of any hashing method in NTPv3 is outside the scope of this Common Criteria evaluation.
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. 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. Administrators can run the "verify <file-location>:/<filename>" command to compare the SHA-512 checksum for any locally stored file with a known-good published checksum.
FPT_TST_EXT.1	The ASAs run 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. The self-testing includes cryptographic algorithm tests (known-answer tests) that feed pre-defined data to cryptographic modules and confirm the resulting output from the modules match expected values, and software integrity tests that compare the checksums of executable code to expected values. The cryptographic algorithm testing (the known-answer tests) verify proper operation of encryption functions, decryption functions, signature padding functions, signature hashing functions, and random number generation. The software integrity tests include checksum verification. Prior to booting to an image, an administrator can verify the integrity of an image file using SHA-512 (refer to FPT_TUD_EXT.1).
FTA_SSL_EXT.1	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.
FTA_SSL.3	
FTA_SSL.4	An administrator is able to exit out of both local and remote administrative sessions, effectively terminating the session so it can't be re-used and will require authentication to establish a new session.
FTA_TAB.1	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 at

TOE SFRs	How the SFR is Satisfied
	the local console or via any remote connection.
FTP_ITC.1	The ASA uses IPsec, SSH, and TLS to protect communications between itself and remote entities for the following purposes: • The ASA protects transmission of audit records when sending syslog message to a remote audit server by transmitting the message over TLS or IPsec. • Connections to authentication servers (AAA servers) can be protected via IPsec tunnels. Connections with AAA servers (via RADIUS and TACACS+) can be configured for authentication of TOE administrators. • SSH sessions can be initiated from the TOE to a remote SSH servers, such as other network devices, for the purposes of remotely administering remote devices. • HTTPS (over TLS) sessions can be initiated from the TOE to a remote TLS-enabled web server for the purposes of uploading or downloading software images or configuration files. Note: In the certified configuration, use of IPsec or TLS VPNs is only approved for tunneling traffic that originates from or terminates at the ASA itself, not for tunneling traffic between hosts across the ASA.
FTP_TRP.1	The ASA uses SSHv2 or TLS/HHTPS (for ASDM) to provide the trusted path (with protection from disclosure and modification) for all remote administration sessions. The ASA also supports tunneling the SSH and ASDM connections in IPsec VPN tunnels (peer-to-peer, or remote VPN client), or TLS VPN tunnels (remote TLS VPN client, or clientless TLS VPN). Note: In the certified configuration, use of IPsec or TLS VPNs is only approved for tunneling traffic that originates from or terminates at the ASA itself, not for tunneling traffic between hosts across the ASA.
Reproduced from the TFFWEP	
FFW_RUL_EXT.1.1 FFW_RUL_EXT.1.6	The ASA provides stateful traffic filtering of IPv4 and IPv6 network traffic. Administratively-defined traffic filter rules (access-lists) can be applied to any interface to filter traffic based on IP parameters including source and destination address, TCP and UDP port numbers, and ICMP source/destination addresses types and codes. The ASA allows establishment of communications between remote endpoints, and tracks the state of each session (e.g. initiating, established, and tear-down), and will clear established sessions after proper tear-down is completed as defined by each protocol, or when session timeouts are reached. To track the statefulness of sessions to/from and through the firewall, the ASA maintains a table of connections in various connection states and connection flags. The ASA updates the table (adding, and removing connections, and modifying states as appropriate) based on configurable connection timeout limits, and by inspecting fields within the packet headers. For further explanation of connection states, see section 8.1. The proper session establishment "handshaking", and termination followed by the ASA is as defined in the following RFCs:

TOE SFRs	How the SFR is Satisfied
	• RFC 792 (ICMPv4) • RFC 4443 (ICMPv6) • RFC 791 (IPv4) • RFC 2460 (IPv6) • TCP, RFC 793, section 2.7 Connection Establishment and Clearing • UDP, RFC 768 (not applicable, UDP is a “stateless” protocol)
FFW_RUL_EXT.1.2, FFW_RUL_EXT.1.3	The TOE supports filtering of the following protocols and enforces proper session establishment, management, and termination as defined in each protocol’s RFC including proper use of: • addresses, type of service, fragmentation data, size and padding, and IP options including loose source routing, strict source routing, and record route as defined in RFC 791 (IPv4), and RFC 2460 (IPv6); • port numbers, sequence and acknowledgement numbers, size and padding, and control bits such as SYN, ACK, FIN, and RST as defined in RFC 793 (TCP); • port numbers, and length as defined in RFC 768 (UDP); and • session identifiers, sequence numbers, types, and codes as defined in RFC 792 (ICMPv4), and RFC 4443 (ICMPv6). Cisco confirms proper implementation of the RFCs through interoperability testing with Cisco and 3rd party products and through protocol compliant testing. The ASA can also support deeper packet inspection and enforce additional RFC compliance beyond session management, but such traffic inspection functionality is not defined within the TFFWEP and is therefore beyond the scope of this CC certification.
FFW_RUL_EXT.1.4, FFW_RUL_EXT.1.5	Each traffic flow control rule on the ASA is defined as either a “permit” rule, or a “deny” rule, and any rule can also contain the keyword “log” which will cause a log message to be generated when a new session is established because it matched the rule. The ASA can be configured to generate a log message for the session establishment of any permitted or denied traffic. When a rule is created to explicitly allow a protocol which is implicitly allowed to spawn additional sessions, the establishment of spawned sessions is logged as well. Access Control Lists (ACLs) are only enforced after they’ve been applied to a network interface. Any network interface can have an ACL applied to it with the “access-group” command, e.g. “access-group sample-acl in interface outside”. Interfaces can be referred to by their identifier (e.g. GigabitEthernet 0/1), or by a name if named using the “nameif” command e.g.: asa(config)# **interface** gigabitethernet0/1 asa(config-if)# **nameif** inside The interface types that can be assigned to an access-group are: • Physical interfaces o Ethernet o GigabitEthernet o TenGigabitEthernet

TOE SFRs	How the SFR is Satisfied
	o Management • Port-channel interfaces (designated by a port-channel number) • Subinterface (designated by the subinterface number) The default state of an interface depends on the type and the context mode: • For the "system" context in single mode or multiple context mode, interfaces have the following default states: o Physical interfaces = Disabled o Subinterfaces = Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled. • For any non-system context (in multiple context mode): All allocated interfaces (allocated to the context by the system context) are enabled by default, no matter what the state of the interface is in the system context. However, for traffic to pass through the interface, the interface also has to be enabled in the system context. If you shut down an interface in the system context, then that interface is down in all contexts to which that interface has been allocated. In interface configuration mode, the administrator can configure hardware settings (for physical interfaces), assign a name, assign a VLAN, assign an IP address, and configure many other settings, depending on the type of interface and the security context mode. For an enabled interface to pass traffic, the following interface configuration mode commands must be used (in addition to explicitly permitting traffic flow by applying and access-group to the interface): "**nameif**", and, for routed mode, "**ip address**". For subinterfaces, also configure the "**vlan**" command. The Management 0/0 interface on the ASA 5512-X through ASA 5555-X has the following characteristics: • No through traffic support • No subinterface support • No priority queue support • No multicast MAC support • If installed into a 5500-X, the IPS SSP software module shares the Management 0/0 interface. Separate MAC addresses and IP addresses are used for the ASA and IPS module, and configuration of the IPS IP address must be performed within the IPS operating system. However, physical characteristics (such as enabling the interface) are configured on the ASA.
FFW_RUL_EXT.1.7	The ASA supports numerous TCP and UDP protocols that require dynamic establishment of secondary network sessions including FTP. The ASA will manage establishment and teardown of the following protocols in accordance with the RFC for each protocol: • FTP (File Transfer Protocol) is a TCP protocol supported in either active or passive mode: o In active mode the client initiates the control session, and the server initiates the data session to a client port provided by the client;

TOE SFRs	How the SFR is Satisfied
	o For active FTP to be allowed through the ASA, the firewall rules must explicitly permit the control session from the client to the server, and "inspect ftp" must be enabled. The ASA will then explicitly permit a control session to be initiated from the client to the server, and implicitly permit data sessions to be initiated from the server to the client while the control session is active. o In passive (PASV) mode, the client initiates the control session, and the client also initiates the data session to a secondary port provided to the client by the server. o For passive FTP to be permitted through the ASA, the firewall rules must explicitly permit the control session from the client to the server, and "inspect ftp" must be enabled with the "match passive-ftp" option enabled. That feature will cause the ASA to look for the PASV or EPSV commands in the FTP control traffic and for the server's destination port, and dynamically permit the data session.
FFW_RUL_EXT.1.8	The ASA can be configured to implement default denial of various mal-formed packets/fragments, and other illegitimate network traffic, and can be configured to log that such packets/frames were dropped. The ASA's IPS functionality can be used to deny and log traffic by defining IPS policies with the "ip audit name" command, specifying the "drop" action, and applying the policy or policies to each enabled interface. Each signature has been classified as either "informational", or "attack". Using the "info" and "attack" keywords in the "ip audit name" command defines the action the ASA will take for each signature classification. asa(config)# **ip audit name** *name* {info | attack} [action [alarm] [drop] [reset]] asa(config)# **ip audit interface** *interface_name policy_name* Example: asa(config)# ip audit name ccpolicy1 attack action alarm reset asa(config)# ip audit name ccpolicy2 info action alarm reset asa(config)# ip audit interface outside ccpolicy1 asa(config)# ip audit interface inside ccpolicy2 Specifying the "alarm" action in addition to the "drop" action will result in generating an audit message when the signature is detected. Messages 400000 through 400051 are Cisco Intrusion Prevention Service signature messages, and have this format: %ASA-4-4000`nn`: IPS:`number string` from `IP_address` to `IP_address` on interface `interface_name` With or without the ASA's IPS functionality enabled, the following traffic will be denied by the TOE, and audit messages will be generated as indicated: 1. packets which are invalid fragments, including IP fragment attack %ASA-2-106020: Deny IP teardrop fragment (size = `number`, offset = `number`) from `IP_address` to `IP_address` %ASA-4-209004: Invalid IP fragment, size = *bytes* exceeds maximum size= `bytes`: src = `source_address`, dest = *dest_address*, proto = *protocol*, id = *number* %ASA-4-402118: IPSEC: Received an *protocol* packet (SPI=*spi*, sequence number *seq_num*) from *remote_IP* (*username*) to *local_IP* containing an illegal IP fragment of length

TOE SFRs	How the SFR is Satisfied
	frag_len with offset *frag_offset*. The following messages will be generated when the ASA's IPS functionality is enabled and configured as described above. %ASA-4-400007: IPS:1100 IP Fragment Attack from *IP_address* to *IP_address* on interface *interface_name* %ASA-4-400009: IPS:1103 IP Overlapping Fragments (Teardrop) from *IP_address* to *IP_address* on interface *interface_name* %ASA-4-400023: IPS:2150 Fragmented ICMP traffic from *IP_address* to *IP_address* on interface *interface_name* %ASA-4-400025: IPS:2154 Ping of Death Attack from *IP_address* to *IP_address* on interface *interface_name* 2. fragmented IP packets which cannot be re-assembled completely; %ASA-4-209003: Fragment database limit of *number* exceeded: src = *source_address*, dest = *dest_address*, proto = *protocol*, id = *number* %ASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set. %ASA-4-423005: Dropped NBDGM *pkt_type_name* fragment with *error_reason_str* from *ifc_name*:*ip_address*/*port* to *ifc_name*:*ip_address*/*port*. %ASA-4-507002: Data copy in proxy-mode exceeded the buffer limit %ASA-7-715060: Dropped received IKE fragment. Reason: *reason* `%ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.` 3. packets where the source address of the network packet is equal to the address of the network interface where the network packet was received; %ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name.* 4. packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received; %ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name.* This next message appears when Unicast RPF has been enabled with the **ip verify reverse-path** command. %ASA-1-106021: Deny *protocol* reverse path check from *source_address* to *dest_address* on interface *interface_name* This next message appears when a packet matching a connection arrived on a different interface from the interface on which the connection began, and the **ip verify reverse-path** command is not configured. %ASA-1-106022: Deny *protocol* connection spoof from *source_address* to *dest_address* on interface *interface_name* 5. packets where the source address of the network packet is defined as

TOE SFRs	How the SFR is Satisfied
	being on a broadcast network; %ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name.* 6. packets where the source address of the network packet is defined as being on a multicast network; %ASA-4-106023: Deny *protocol* src [*interface_name*:*source_address/source_port*] dst i*nterface_name*:*dest_address/dest_port* [type {*string*}, code {*code*}] by access_group *acl_ID* The preceding message will be generated when the rules listed below are configured without the “log” option. %ASA-4-106100: access-list *acl_ID* denied *protocol* *interface_name*/*source_address*(*source_port*) - *interface_name*/*dest_address*(*dest_port*) hit-cnt *number* ({first hit | *number*-secondinterval}) hash codes The preceding message will be generated when these rules are configured with the “log” option: asa(config)#**object-group network** *grp_name* asa(config-network-object-group)#**network-object** 224.0.0.0 255.0.0.0 #IPv4 multicast asa(config-network-object-group)#**network-object** FF00::/8 #IPv6 multicast asa(config)#**access-list** *acl-name* **extended deny ip** *grp-name* **any [log]** asa(config)#**access-group in interface** *int-name* 7. packets where the source address of the network packet is defined as being a loopback address; %ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name.* The preceding message will be generated when no ACL has been defined to explicitly deny this traffic. %ASA-4-106023: Deny *protocol* src [*interface_name*:*source_address/source_port*] dst i*nterface_name*:*dest_address/dest_port* [type {*string*}, code {*code*}] by access_group *acl_ID* The preceding message will be generated when the rules listed below are configured without the “log” option. %ASA-4-106100: access-list *acl_ID* denied *protocol* *interface_name*/*source_address*(*source_port*) - *interface_name*/*dest_address*(*dest_port*) hit-cnt *number* ({first hit | *number*-secondinterval}) hash codes The preceding message will be generated when these rules are configured with the “log” option: asa(config)#**object-group network** *grp_name* asa(config-network-object-group)#**network-object** 127.0.0.0 255.0.0.0 #IPv4 loopback asa(config-network-object-group)#**network-object** ::1/128 #IPv6 loopback asa(config)#**access-list** *acl-name* **extended deny ip** *grp-name* **any [log]**

TOE SFRs	How the SFR is Satisfied
	asa(config)#**access-group in interface** *int-name* *8.* packets where the source address of the network packet is a multicast; See item number 6. *9.* packets where the source or destination address of the network packet is a link-local address; %ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name.* The preceding message will be generated when no ACL has been defined to explicitly deny this traffic. %ASA-4-106023: Deny *protocol* src [*interface_name*:*source_address/source_port*] dst i*nterface_name*:*dest_address/dest_port* [type {*string*}, code {*code*}] by access_group *acl_ID* The preceding message will be generated when the rules listed below are configured without the "log" option. %ASA-4-106100: access-list *acl_ID* denied *protocol* *interface_name*/*source_address*(*source_port*) - *interface_name*/*dest_address*(*dest_port*) hit-cnt *number* ({first hit | *number*-secondinterval}) hash codes The preceding message will be generated when these rules are configured with the "log" option: asa(config)#**object-group network** *grp_name* asa(config-network-object-group)#**network-object** 127.0.0.0 255.0.0.0 #IPv4 link-local asa(config-network-object-group)#**network-object** FE80::/10 #IPv6 link-local asa(config)#**access-list** *acl-name* **extended deny ip** *grp-name* **any [log]** asa(config)#**access-list** *acl-name* **extended deny ip any** *grp-name* **[log]** asa(config)#**access-group in interface** *int-name* *10.* packets where the source or destination address of the network packet is defined as being an address "reserved for future use" as specified in RFC 5735 for IPv4; %ASA-4-106023: Deny *protocol* src [*interface_name*:*source_address/source_port*] dst i*nterface_name*:*dest_address/dest_port* [type {*string*}, code {*code*}] by access_group *acl_ID* The preceding message will be generated when the rules listed below are configured without the "log" option. %ASA-4-106100: access-list *acl_ID* denied *protocol* *interface_name*/*source_address*(*source_port*) - *interface_name*/*dest_address*(*dest_port*) hit-cnt *number* ({first hit | *number*-secondinterval}) hash codes The preceding message will be generated when these rules are configured with the "log" option: asa(config)#**object-group network** *grp_name* asa(config-network-object-group)#**network-object** 192.0.0.0 255.0.0.0 #IPv4 reserved

TOE SFRs	How the SFR is Satisfied
	asa(config-network-object-group)#**network-object** 240.0.0.0 128.0.0.0 #IPv4 reserved asa(config)#**access-list** *acl-name* **extended deny ip** *grp-name* **any [log]** asa(config)#**access-list** *acl-name* **extended deny ip any** *grp-name* **[log]** asa(config)#**access-group in interface** *int-name* *11.* packets where the source or destination address of the network packet is defined as an "unspecified address" or an address "reserved for future definition and use" as specified in RFC 3513 for IPv6; %ASA-4-106023: Deny *protocol* src [*interface_name*:*source_address/source_port*] dst *interface_name*:*dest_address/dest_port* [type {*string*}, code {*code*}] by access_group *acl_ID* The preceding message will be generated when the rules listed below are configured without the "log" option. %ASA-4-106100: access-list *acl_ID* denied *protocol* *interface_name*/*source_address*(*source_port*) -*interface_name*/*dest_address*(*dest_port*) hit-cnt *number* ({first hit | *number*-secondinterval}) hash codes The preceding message will be generated when these rules are configured with the "log" option: asa(config)#**object-group network** *grp_name* asa(config-network-object-group)#**network-object** :: #IPv6 unspecified asa(config-network-object-group)#**network-object** 0000::/8 #IPv6 reserved asa(config)#**access-list** *acl-name* **extended deny ip** *grp-name* **any [log]** asa(config)#**access-list** *acl-name* **extended deny ip any** *grp-name* **[log]** asa(config)#**access-group in interface** *int-name* *12.* Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified; %ASA-6-106012: Deny IP from *IP_address* to *IP_address*, IP options *hex*. The following messages will be generated when the ASA's IPS functionality is enabled and configured as described above. %ASA-4-400001: IPS:1001 IP options-Record Packet Route from *IP_address* to *IP_address* on interface *interface_name* %ASA-4-400004: IPS:1004 IP options-Loose Source Route from *IP_address* to *IP_address* on interface *interface_name* %ASA-4-400006: IPS:1006 IP options-Strict Source Route from *IP_address* to *IP_address* on interface *interface_name* *13.* By default, ASA will also drop (and is capable of logging) a variety of other IP packets with invalid content including: • Invalid source and/or destination IP address including: o source or destination is the network address (e.g. 0.0.0.0) o source and destination address are the same (with or without the source and destination ports being the same) o first octet of the source IP is equal to zero

TOE SFRs	How the SFR is Satisfied
	o network part of the source IP is equal to all zeros or all ones o host part of the source IP is equal to all zeros or all ones • Invalid ICMP packets including: sequence number mismatch; invalid ICMP code, and ICMP responses unrelated to any established ICMP session
FFW_RUL_EXT.1.9	ASA administrators have control over the sequencing of access control entries (ACEs) within an access control list (ACL) to be able to set the sequence in which ACEs are applied within any ACL. The entries within an ACL are always applied in a top-down sequence, and the first entry that matches the traffic is the one that's applied, regardless of whether there may be a more precise match for the traffic further down in the ACL. By changing the ordering/numbering of entries within an ACL, the administrator chances the sequence in which the entries are compared to network traffic flows.
FFW_RUL_EXT.1.10	An implicit "deny-all" rule is applied to all interfaces to which any traffic filtering rule has been applied. The implicit deny-all rule is executed after all admin-defined rules have been executed, and will result in dropping all traffic that has not been explicitly permitted, or explicitly denied. If an administrator wants to log all denied traffic, a rule entry should be added that denies all traffic and logs it, e.g. "access-list sample-acl deny ip any any log". During initialization/startup (while the ASA is booting) the configuration has yet to be loaded, and no traffic can flow through any of its interfaces. No traffic can flow through the ASA interfaces until the POST has completed, and the configuration has been loaded. If any aspect of the POST fails during boot, the ASA will reload without forwarding traffic. If a critical component of the ASA, such as the clock or cryptographic modules, fails while the ASA is in an operational state, the ASA will reload, which stops the flow of traffic. If a component such as a network interface, which is not critical to the operation of the ASA, but may be critical to one or more traffic flows, fails while the ASA is operational, the ASA will continue to function, though all traffic flows through the failed network interface(s) will be dropped.

6.2 TOE Bypass and interference/logical tampering Protection Measures

The TOE consists of a hardware platform in which all operations in the TOE scope are protected from interference and tampering by untrusted subjects. All administration and configuration operations are performed within the physical boundary of the TOE. Also, 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. There are no undocumented interfaces for managing the product.

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

No processes outside of the TOE are allowed direct access to any TOE memory. The TOE only accepts traffic through legitimate TOE interfaces. Specifically, processes outside the TOE are not able to execute code on the TOE. None of these interfaces provide any access to internal TOE resources.

Finally, the TOE enforces information flow control policies through firewall rules and IPsec 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. Traffic flows characterized as unauthorized are discarded and not permitted to circumvent the TSF. There are no unmediated traffic flows into or out of the TOE. During startup, the interfaces of the TOE are not operational (will not allow inbound, outbound, or through-the-box traffic) until after the Power-On Self-Test (POST) completes, and the startup configuration has been loaded. The loading of the startup configuration puts the TOE it its evaluated configuration all its administratively-defined traffic flow control policies (access-lists), and applies the access-lists to interfaces before the interfaces are enabled.

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. When failures occur in hardware components, such as Network Interface Cards (NICs), the NIC may cease to forward traffic, but the software components of the TOE (such as traffic filtering, I&A, and auditing) continue to operated. When failures occur in software components, the TOE will crash (stopping all traffic flow), and attempt to reload to ensure that no security-relevant operations can be performed while the TOE security functions are not fully operational.

7 RATIONALE

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined within the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) and Traffic Filter Firewall Extended Package (TFFWEP) and NDPP and TFFWEP.

7.1 Security objectives rationale

The security objectives rationale shows how the security objectives correspond to assumptions, threats, and organizational security policies and provide a justification of that tracing.

7.1.1 Tracing of security objectives to SPD

The tracing shows how the security objectives O.* and OE.* trace back to assumptions A.*, threats T.*, and organizational security policies OSP.* defined by the SPD.

Table 17 Tracing of security objectives to SPD

	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN	A.CONNECTIONS	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.ADMIN_ERROR	T.UNDETECTED_ACTIONS	T.RESOURCE_EXHAUSTION	T.USER_DATA_REUSE	T.TSF_FAILURE	T.MEDIATE	T.TRANSMIT	T.NETWORK_DISCLOSURE	T. NETWORK_ACCESS	T.NETWORK_MISUSE	T.NETWORK_DOS	P.ACCESS BANNER
Objectives from NDPP																		
O.PROTECTED_COMMUNICATIONS													X					
O.VERIFIABLE_UPDATES						X												
O.SYSTEM_MONITORING								X								X		
O.DISPLAY_BANNER																		X
O.TOE_ADMINISTRATION							X											
O.RESIDUAL_INFORMATION_CLEARING										X								
O.RESOURCE_AVAILABILITY									X									
O.SESSION_LOCK					X													
O.TSF_SELF_TEST											X							
OE.NO_GENERAL_PURPOSE	X																	
OE.PHYSICAL		X																
OE.TRUSTED_ADMIN			X															
Additional Objectives from TFFWEP																		
O.ADDRESS_FILTERING														X	X	X	X	
O.PORT_FILTERING														X	X	X	X	

	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN	A.CONNECTIONS	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.ADMIN_ERROR	T.UNDETECTED_ACTIONS	T.RESOURCE_EXHAUSTION	T.USER_DATA_REUSE	T.TSF_FAILURE	T.MEDIATE	T.TRANSMIT	T.NETWORK_DISCLOSURE	T. NETWORK_ACCESS	T.NETWORK_MISUSE	T.NETWORK_DOS	P.ACCESS BANNER
O.RELATED_CONNECTION _FILTERING															X			
O.STATEFUL_INSPECTION																	X	
OE.CONNECTIONS				X														

7.1.2 Justification of tracing

The justification demonstrates that the tracing of the security objectives to assumptions, threats, and OSPs is effective and all the given assumptions are upheld, all the given threats are countered, and all the given OSPs are enforced.

7.1.2.1 Tracing of assumptions

Table 18 Assumptions Rationale

Environment Objective	Rationale
OE.NO_GENERAL_PURPOSE	This security objective is necessary to address the assumption A.NO_GENERAL_PURPOSE by ensuring there are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) capabilities on the TOE.
OE.PHYSICAL	This security objective is necessary to address the assumption A.PHYSICAL by ensuring the TOE and the data it contains is physically protected from unauthorized access.
OE.TRUSTED_ADMIN	This security objective is necessary to address the assumption A.TRUSTED_ADMIN by ensuring the administrators are non-hostile and follow all administrator guidance.

7.1.2.2 Tracing of threats and OSPs

Table 19 Threat and OSP Rationale

Objective	Rationale
Security Objectives Drawn from NDPP	
O.PROTECTED_COMMUNICATIONS	This security objective is necessary to counter the threat: T.TRANSMIT to ensure the communications with the TOE is not compromised

Objective	Rationale
O.VERIFIABLE_UPDATES	This security objective is necessary to counter the threat T.UNAUTHORIZED_UPDATE to ensure the end user has not installed a malicious update, thinking that it was legitimate.
O.SYSTEM_MONITORING	This security objective is necessary to counter the T.UNDETECTED_ACTIONS to ensure activity is monitored so the security of the TOE is not compromised.
O.DISPLAY_BANNER	This security objective is necessary to address the Organization Security Policy P.ACCESS_BANNER to ensure an advisory notice and consent warning message regarding unauthorized use of the TOE is displayed before the session is established.
O.TOE_ADMINISTRATION	This security objective is necessary to counter the T.ADMIN_ERROR that ensures actions performed on the TOE are logged so that indications of a failure or compromise of a TOE security mechanism are known and corrective actions can be taken.
O.RESIDUAL_INFORMATION_CLEARING	This security objective is necessary to counter the threat T.USER_DATA_REUSE so that data traversing the TOE could inadvertently be sent to a user other than that intended by the sender of the original network traffic.
O.RESOURCE_AVAILABILITY	This security objective is necessary to counter the threat: T.RESOURCE_EXHAUSTION to mitigate a denial of service, thus ensuring resources are available.
O.SESSION_LOCK	This security objective is necessary to counter the threat: T.UNAUTHORIZED_ACCESS to ensure accounts cannot be compromised and used by an attacker that does not otherwise have access to the TOE.
O.TSF_SELF_TEST	This security objective is necessary to counter the threat T.TSF_FAILURE to ensure failure of mechanisms do not lead to a compromise in the TSF.
Security Objectives Drawn from TFFWEP	
O.ADDRESS_FILTERING	This security objective is necessary to counter the threats: T.NETWORK_DISCLOSURE, T. NETWORK_ACCESS, T.NETWORK_MISUSE, T.NETWORK_DOS to ensure the TOE will provide the means to filter and log network packets based on source and destination addresses.
O.PORT_FILTERING	This security objective is necessary to counter the threats: T.NETWORK_DISCLOSURE, T. NETWORK_ACCESS, T.NETWORK_MISUSE, T.NETWORK_DOS to ensure the TOE will provide the means to filter and log network packets based on source and destination transport layer ports.
O.RELATED_CONNECTION_FILTERING	This security objective is necessary to counter the threat T.NETWORK_ACCESS to ensure for specific protocols, the TOE will dynamically permit a network packet flow in response to a connection permitted by the ruleset.
O.STATEFUL_INSPECTION	This security objective is necessary to address the threat T.NETWORK_DOS to ensure the TOE will determine if a network packet belongs to an allowed established connection before applying the ruleset.

7.1.3 Security objectives conclusion

The tracing of the security objectives to assumptions, threats, and OSPs, and the justification of that tracing showed that all the given assumptions are upheld, all the given threats are countered, all the given OSPs are enforced, and the security problem as defined in the SPD is solved.

7.2 Rationale for requirements/TOE Objectives

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, the tables below illustrate the mapping between the security requirements and the security objectives and the relationship between the threats, policies and IT security objectives. The functional and assurance requirements presented in the NDPP and TFFWEP are mutually supportive and their combination meets the stated security objectives.

7.3 Rationale for TOE Security Objectives

Table 20: SFR/Objectives Mappings

	O.PROTECTED_COMMUNICATIONS	O.VERIFIABLE_UPDATES	O.SYSTEM_MONITORING	O.DISPLAY_BANNER	O.TOE_ADMINISTRATION	O.RESIDUAL_INFORMATION_CLEARING	O.RESOURCE_AVAILABILITY	O.SESSION_LOCK	O.TSF_SELF_TEST	O.MEDIATE	O.ADDRESS_FILTERING	O.PORT_FILTERING	O.RELATED_CONNECTION_FILTERING	O.STATEFUL_INSPECTION
SFRs Drawn from NDPP														
FAU_GEN.1			X											
FAU_GEN.2			X											
FAU_STG_EXT.1			X											
FCS_CKM.1	X													
FCS_CKM_EXT.4	X													
FCS_COP.1(1)	X													
FCS_COP.1(2)	X	X												
FCS_COP.1(3)	X	X												
FCS_COP.1(4)	X													
FCS_HTTPS_EXT.1	X													
FCS_IPSEC_EXT.1	X													
FCS_SSH_EXT.1	X													
FCS_RBG_EXT.1	X													
FCS_TLS_EXT.1	X													
FDP_RIP.2						X								
FIA_PMG_EXT.1														

	O.PROTECTED_COMMUNICATIONS	O.VERIFIABLE_UPDATES	O.SYSTEM_MONITORING	O.DISPLAY_BANNER	O.TOE_ADMINISTRATION	O.RESIDUAL_INFORMATION_CLEARING	O.RESOURCE_AVAILABILITY	O.SESSION_LOCK	O.TSF_SELF_TEST	O.MEDIATE	O.ADDRESS_FILTERING	O.PORT_FILTERING	O.RELATED_CONNECTION_FILTERING	O.STATEFUL_INSPECTION
FIA_UIA_EXT.1					X									
FIA_UAU_EXT.2					X									
FIA_UAU.7					X									
FMT_MTD.1					X									
FMT_SMF.1					X									
FMT_SMR.2					X									
FPT_SKP_EXT.1	X													
FPT_APW_EXT.1	X													
FPT_STM.1			X											
FPT_TUD_EXT.1		X												
FPT_TST_EXT.1									X					
FTA_SSL_EXT.1								X						
FTA_SSL.3								X						
FTA_SSL.4								X						
FTA_TAB.1				X										
FTP_ITC.1	X													
FTP_TRP.1	X													
SFRs drawn from TFFWEP														
FFW_RUL_EXT.1											X	X	X	X

The inspection of Table 20 shows that:

- Each SFR traces back to at least one security objective;
- Each security objective for the TOE has at least one SFR tracing to it.

7.3.1.1 Justification of SFR tracing

The justification demonstrates that the SFRs address all security objectives of the TOE.

Table 21 SFR Tracing Justification

Objective	Rationale
Objectives Drawn from NDPP	
O.PROTECTED_COMMUNICATIONS	The SFRs, FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_HTTPS_EXT.1, FCS_IPSEC_EXT.1, FCS_SSH_EXT.1, FCS_RBG_EXT.1,

Objective	Rationale
	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1, FPT_PTD_EXT.1(2), FPT_RPL.1, FTP_ITC.1, FTP_TRP.1 meet this objective by ensuring the communications between the TOE and endpoints are secure by implementing the encryption protocols as defined in the SFRs and as specified by the RFCs.
O.VERIFIABLE_UPDATES	The SFRs, FPT_TUD_EXT.1, FCS_COP.1(2), FCS_COP.1(3) meet this objective by ensuring the update was downloaded via secure communications, is from a trusted source, and the update can be verified by cryptographic mechanisms prior to installation.
O.SYSTEM_MONITORING	The SFRs, FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1, FPT_STM.1 meet this objective by auditing actions on the TOE. The audit records identify the user associated with the action/event, whether the action/event was successful or failed, the type of action/event, and the date/time the action/event occurred. The audit logs are transmitted securely to a remote syslog server. If connectivity to the remote syslog server is lost, the TOE will block new permit actions.
O.DISPLAY_BANNER	The SFR, FTA_TAB.1 meets this objective by displaying an advisory notice and consent warning message regarding unauthorized use of the TOE.
O.TOE_ADMINISTRATION	The SFRs, FIA_UIA_EXT.1, FIA_PMG_EXT.1, FIA_UAU_EXT.5, FIA_UAU.6, FIA_UAU.7, FMT_MOF.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SFR.1, FPT_PTD_EXT.1(1), FTA_SSL_EXT.1, FTA_SSL.3 meet this objective by ensuring the TOE supports a password-based authentication mechanism with password complexity enforcement such as, strong passwords, password life-time constraints, providing current password when changing the password, obscured password feedback when logging in, and passwords are not stored in plaintext. The objective is further met by ensuring restrictive default values are enforced on the SFPs (authorization and flow control), that only authorized administrators to override the default values, that the TOE provides the management and configuration features to securely manage the TOE and that those functions are restricted to the authorized administrator, and the implementation of session termination after an administrative configurable inactivity time period whereas the user must be re-authenticated. In addition, the TOE provides the ability for an authorized administrator to exit or logoff an administrator session. The TOE must also protects itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. The TOE will provide the authorized administrators the capability to review Audit data. Security relevant events must be available for review by authorized administrators as provided by FAU_SAR.1. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to delete audit data stored locally on the TOE as provided by FAU_STG.1.
O.RESIDUAL_INFORMATION_ CLEARING	The SFR, FDP_RIP.2 meets this objective by ensuring no left over user data from the previous transmission is included in the network traffic.
O.RESOURCE_AVAILABILITY	The SFR, FRU_RSA.1 meets this objective by limiting the number of amount of exhaustible resources, such the number of concurrent administrative sessions.
O.SESSION_LOCK	The SFRs, FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4 meet this objective by terminating a session due to meeting/exceeding the inactivity time limit. In addition, the TOE allows an authorized administrator to exit or logoff an administrator session.

Objective	Rationale
O.TSF_SELF_TEST	The SFR, FPT_TST_EXT.1 meets this objective by performing self-test to ensure the TOE is operating correctly and all functions are available and enforced.
Reproduced from the TFFWEP	
O.ADDRESS_FILTERING	The SFR, FFW_RUL_EXT.1 meets this objective by ensuring no left over user data from the previous transmission is included in the network traffic.
O.PORT_FILTERING	The SFR, FFW_RUL_EXT.1 meets this objective by providing the means to filter and log network packets based on source and destination transport layer ports.
O.STATEFUL_INSPECTION	The SFR, FFW_RUL_EXT.1 meets this objective by determine if a network packet belongs to an allowed established connection before applying the ruleset.
O.RELATED_CONNECTION_FILTERING	The SFR, FFW_RUL_EXT.1 meets this objective by dynamically permitting a network packet flow in response to a connection permitted by the ruleset.

8 Supplemental TOE Summary Specification Information

8.1 Tracking of Stateful Firewall Connections

8.1.1 Establishment and Maintenance of Stateful Connections

As network traffic enters an interface of the ASA, the ASA inspects the packet header information to determine whether the packet is allowed by access control lists, and whether an established connection already exists for that specific traffic flow. The ASA maintains and continuously updates connection state tables to keep tracked of establishment, teardown, and open sessions. To help determine whether a packet can be part of a new session or an established session, the ASA uses information in the packet header and protocol header fields to determine the session state to which the packet applies as defined by the RFC for each protocol.

8.1.2 Viewing Connections and Connection States

To display the connection state for the designated connection type, use the **show conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses. The syntax is:

show conn [**count** | [**all**] [**detail**] [**long**] [**state** *state_type*] [**protocol** {**tcp** | **udp**}] [**scansafe**] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*]] [**user-identity** | **user** [*domain_nickname*\]*user_name* | **user-group** [*domain_nickname*\\]*user_group_name*] | **security-group**]

The **show conn** command displays the number of active TCP and UDP connections, and provides information about connections of various types. By default, the output of "**show conn**" shows only the through-the-ASA connections. To include connections to/from the ASA itself in the command output, add the **all** keyword, "**show conn all**".

Table 22: Syntax Description

address	(Optional) Displays connections with the specified source or destination IP address.
all	(Optional) Displays connections that are to the device or from the device, in addition to through-traffic connections.
count	(Optional) Displays the number of active connections.
dest_ip	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: 10.1.1.1-10.1.1.5
dest_port	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-). For example: 1000-2000
detail	(Optional) Displays connections in detail, including translation type and interface information.
long	(Optional) Displays connections in long format.

netmask *mask*	(Optional) Specifies a subnet mask for use with the given IP address.
port	(Optional) Displays connections with the specified source or destination port.
protocol {**tcp** | **udp**}	(Optional) Specifies the connection protocol, which can be **tcp** or **udp**.
scansafe	(Optional) Shows connections being forwarded to the Cloud Web Security server.
security-group	(Optional) Specifies that all connections displayed belong to the specified security group.
src_ip	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: 10.1.1.1-10.1.1.5
src_port	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-). For example: 1000-2000
state *state_type*	(Optional) Specifies the connection state type. See Table 46-5 for a list of the keywords available for connection state types.
user [*domain_nickname*\] *user_name*	(Optional) Specifies that all connections displayed belong to the specified user. When you do not include the *domain_nickname* argument, the ASA displays information for the user in the default domain.
user-group [*domain_nickname*\\] *user_group_name*	(Optional) Specifies that all connections displayed belong to the specified user group. When you do not include the *domain_nickname* argument, the ASA displays information for the user group in the default domain.
user-identity	(Optional) Specifies that the ASA display all connections for the Identity Firewall feature. When displaying the connections, the ASA displays the user name and IP address when it identifies a matching user. Similarly, the ASA displays the host name and an IP address when it identifies a matching host.

The connection types that you can specify using the **show conn state** command are defined in the table below. When specifying multiple connection types, use commas without spaces to separate the keywords.

Table 23: Connection State Types

Keyword	**Connection Type Displayed**
up	Connections in the up state.
conn_inbound	Inbound connections.
ctiqbe	CTIQBE connections
data_in	Inbound data connections.
data_out	Outbound data connections.
finin	FIN inbound connections.
finout	FIN outbound connections.
h225	H.225 connections
h323	H.323 connections
http_get	HTTP get connections.
mgcp	MGCP connections.
nojava	Connections that deny access to Java applets.

rpc	RPC connections.
service_module	Connections being scanned by an SSM.
sip	SIP connections.
skinny	SCCP connections.
smtp_data	SMTP mail data connections.
sqlnet_fixup_data	SQL*Net data inspection engine connections.
tcp_embryonic	TCP embryonic connections.
vpn_orphan	Orphaned VPN tunneled flows.

When using the **detail** option, the ASA displays information about the translation type and interface information using the connection flags defined in the table below.

Table 24: Connection State Flags

Flag	Description
a	awaiting outside ACK to SYN
A	awaiting inside ACK to SYN
b	TCP state bypass. By default, all traffic that passes through the Cisco Adaptive Security Appliance (ASA) is inspected using the Adaptive Security Algorithm and is either allowed through or dropped based on the security policy. In order to maximize the firewall performance, the ASA checks the state of each packet (for example, is this a new connection or an established connection?) and assigns it to either the session management path (a new connection SYN packet), the fast path (an established connection), or the control plane path (advanced inspection). TCP packets that match existing connections in the fast path can pass through the adaptive security appliance without rechecking every aspect of the security policy. This feature maximizes performance.
B	initial SYN from outside
C	Computer Telephony Interface Quick Buffer Encoding (CTIQBE) media connection
d	dump
D	DNS
E	outside back connection. This is a secondary data connection that must be initiated from the inside host. For example, using FTP, after the inside client issues the PASV command and the outside server accepts, the ASA preallocates an outside back connection with this flag set. If the inside client attempts to connect back to the server, then the ASA denies this connection attempt. Only the outside server can use the preallocated secondary connection.
f	inside FIN
F	outside FIN
g	Media Gateway Control Protocol (MGCP) connection
G	connection is part of a group The G flag indicates the connection is part of a group. It is set by the GRE and FTP Strict fixups to designate the control connection and all its associated secondary connections. If the control connection terminates, then all associated secondary connections are also terminated.
h	H.225
H	H.323
i	incomplete TCP or UDP connection
I	inbound data

k	Skinny Client Control Protocol (SCCP) media connection
K	GTP t3-response
m	SIP media connection
M	SMTP data
O	outbound data
p	replicated (unused)
P	inside back connection This is a secondary data connection that must be initiated from the inside host. For example, using FTP, after the inside client issues the PORT command and the outside server accepts, the ASA preallocates an inside back connection with this flag set. If the outside server attempts to connect back to the client, then the ASA denies this connection attempt. Only the inside client can use the preallocated secondary connection.
q	SQL*Net data
r	inside acknowledged FIN
R	If TCP: outside acknowledged FIN for TCP connection If UDP: UDP RPC2 Because each row of “show conn” command output represents one connection (TCP or UDP), there will be only one R flag per row.
s	awaiting outside SYN
S	awaiting inside SYN
t	SIP transient connection For a UDP connection, the value t indicates that it will timeout after one minute.
T	SIP connection For UDP connections, the value T indicates that the connection will timeout according to the value specified using the “timeout sip” command.
U	up
V	VPN orphan
W	WAAS
X	Inspected by the service module, such as a CSC SSM.
y	For clustering, identifies a backup owner flow.
Y	For clustering, identifies a director flow.
z	For clustering, identifies a forwarder flow.
Z	Cloud Web Security

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by *app_id*, and the idle timer for each app_id runs independently. Because the app_id expires independently, a legitimate DNS response can only pass through the ASA within a limited period of time and there is no resource build-up. However, when the **show conn** command is entered, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

When the ASA creates a pinhole to allow secondary connections, this is shown as an incomplete conn by the **show conn** command. Incomplete connections will be cleared from the connections table when they reach their timeout limit, and can be cleared manually by using the "**clear conn"** command. When there is no TCP traffic for the period of inactivity defined by the **timeout conn** command (by default, 1:00:00), the connection is closed and the corresponding conn flag entries are no longer displayed.

If a LAN-to-LAN/Network-Extension Mode tunnel drops and does not come back, there might be a number of orphaned tunnel flows. These flows are not torn down as a result of the tunnel going down, but all the data attempting to flow through them is dropped. The **show conn** command output shows these orphaned flows with the **V** flag.

Table 25: TCP connection directionality flags

Flag	Description
B	Initial SYN from outside
a	Awaiting outside ACK to SYN
A	Awaiting inside ACK to SYN
f	Inside FIN
F	Outside FIN
s	Awaiting outside SYN
S	Awaiting inside SYN

8.1.3 Examples

The following is sample output from the **show conn** command. This example shows a TCP session connection from inside host 10.1.1.15 to the outside Telnet server at 10.10.49.10. Because there is no B flag, the connection is initiated from the inside. The "U", "I", and "O" flags denote that the connection is active and has received inbound and outbound data.

```
hostname# show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti

TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0, flags Ti
```

The following is sample output from the **show conn detail** command. This example shows a UDP connection from outside host 10.10.49.10 to inside host 10.1.1.15. The D flag denotes that this is a DNS connection. The number 1028 is the DNS ID over the connection.

```
hostname# show conn detail

54 in use, 123 most used

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,

    B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,

    D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,

    G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,

    i - incomplete, J - GTP, j - GTP data, K - GTP t3-response

    k - Skinny media, M - SMTP data, m - SIP media, n - GUP

    O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,

    q - SQL*Net data, R - outside acknowledged FIN,

    R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,

    s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,

    V - VPN orphan, W - WAAS,

    X - inspected by service module

TCP outside:10.10.49.10/23 inside:10.1.1.15/1026, flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435

UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028, flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435

TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060, flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435

TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060, flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346

TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000, flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464

TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000, flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156

TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000, flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405

TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060, flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129

TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060, flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529

TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000, flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718

TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000, flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694

TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000, flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742

TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000, flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582

TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000, flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

8.2 Key Zeroization

The following table describes the key zeroization referenced by FCS_CKM_EXT.4 provided by the TOE.

Table 26: TOE Key Zeroization

Critical Security Parameters (CSPs)	Zeroization Cause and Effect
Diffie-Hellman Shared Secret	Automatically zeroized after completion of DH exchange, by calling a specific API within the two crypto modules, when module is shutdown, or reinitialized. Overwritten with: 0x00
Diffie Hellman private exponent	Automatically zeroized upon completion of DH exchange, by calling a specific API within the two crypto modules, and when module is shutdown, or reinitialized. Overwritten with: 0x00
SSH Private Key	Automatically zeroized upon generation of a new key Overwritten with: 0x00
SSH Session Key	Automatically zeroized when the SSH session is terminated. Overwritten with: 0x00
RSA Private Key	Automatically when a new RSA key is generated, or when an administrator enters the “crypto key zeroize rsa” command. Overwritten with: 0x00
All CSPs	Zeroized on-demand on all file systems via the “erase” command.

8.3 NIST Special Publication 800-56B

The TOE is compliant with NIST SP 800-56B as described in Table 27 below.

Table 27 800-56B Compliance

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
5 Cryptographic Elements	None.	None.	Yes	N/A

[1] This column does not included “should/should not” statements that relate to the “owner”, “recipient”, “application”, or “party” as they are outside of the scope of the TOE.

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
5.1 Cryptographic Hash Functions	None.	None.	Yes	N/A
5.2 Message Authentication Code (MAC) Algorithm	None.	None.	Yes	N/A
5.2.1 MacTag Computation	None.	None.	Yes	N/A
5.2.2 MacTag Checking	N/A, no shall statements	None.	Yes	N/A
5.2.3 Implementation Validation Message	None.	None.	Yes	N/A
5.3 Random Bit Generation	None.	None.	Yes	N/A
5.4 Prime Number Generators	Only approved prime number generation methods shall be employed in this Recommendation.	None.	No	TOE is ANSI X9.31 compliant.
5.5 Primality Testing Methods	None.	None.	Yes	N/A
5.6 Nonces	None.	"When using a nonce, a random nonce **should** be used."	Yes	N/A
5.7 Symmetric Key-Wrapping Algorithms	N/A for TLS and SSH.	None.	Yes	N/A
5.8 Mask Generation Function (MGF)	None.	None.	Yes	N/A
5.9 Key Derivation Functions for Key Establishment Schemes	None.	None.	Yes	TOE uses other allowable methods and the protocols as referenced in FIPS 140-2 Annex D
5.9.1 Concatenation Key Derivation Function (Approved Alternative 1)	None.	None.	Yes	N/A
5.9.2 ASN.1 Key	None.	None.	Yes	N/A

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
Derivation Function (Approved Alternative 2)				
6 RSA Key Pairs	N/A, no shall statements	None.	Yes	N/A
6.1 General Requirements	None.	"a key pair used for schemes specified in this recommendation **should not** be used for any schemes not specified herein"	Yes	N/A
6.2 Criteria for RSA Key Pairs for Key Establishment	N/A, no shall statements	None.	Yes	N/A
6.2.1 Definition of a Key Pair	None.	None.	Yes	N/A
6.2.2 Formats	N/A, no shall statements	None.	Yes	N/A
6.2.3 Parameter Length Sets	None.	"The MacKey length shall meet or exceed the target security strength, and **should** meet or exceed the security strength of the modulus."	Yes	N/A
6.3 RSA Key Pair Generators	None.	None.	Yes	N/A
6.3.1 RSAKPG1 Family: RSA Key Pair Generation with a Fixed Public Exponent	No shall statements (def of approved key pair generator)	None.	Yes	N/A
6.3.2 RSAKPG2 Family: RSA Key Pair Generation with a Random Public Exponent	No shall statements (def of approved key pair generator)	None.	Yes	N/A
6.4 Assurances of Validity	N/A, no shall statements	None.	Yes	N/A
6.4.1 Assurance of Key Pair Validity	None.	None.	Yes	N/A
6.4.2 Recipient Assurances of Public	None.	None.	Yes	N/A

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
Key Validity				
6.5 Assurances of Private Key Possession	None.	None.	Yes	N/A
6.5.1 Owner Assurance of Private Key Possession	None.	None.	Yes	N/A
6.5.2 Recipient Assurance of Owner's Possession of a Private Key	None.	None.	Yes	N/A
6.6 Key Confirmation	None.	None.	Yes	N/A
6.6.1 Unilateral Key Confirmation for Key Establishment Schemes	Unilateral Key Confirmation is done for both TLS and SSH, however it varies slightly from that outlined here.	None.	Yes	N/A
6.6.2 Bilateral Key Confirmation for Key Establishment Schemes	N/A, no shall statements	None.	Yes	N/A
6.7 Authentication	N/A, no shall statements	None.	Yes	N/A
7 IFC Primitives and Operations	N/A, no shall statements	None.	Yes	N/A
7.1 Encryption and Decryption Primitives	N/A, no shall statements	None.	Yes	N/A
7.1.1 RSAEP	N/A, no shall statements	None.	Yes	N/A
7.1.2 RSADP	N/A, no shall statements	"Care **should** be taken to ensure that an implementation of RSADP does not reveal even partial information about the value of k."	Yes	N/A
7.2 Encryption and Decryption Operations	N/A, no shall statements	None.	Yes	N/A

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
7.2.1 RSA Secret Value Encapsulation (RSASVE)	N/A, no shall statements	"Care **should** be taken to ensure that an implementation does not reveal information about the encapsulated secret value Z." "the observable behavior of the I2BS routine should not reveal even partial information about the byte string Z."	Yes	N/A
7.2.2 RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP)	None.	"Care should be taken to ensure that the different error conditions that may be detected in Step 5 above cannot be distinguished from one another by an opponent, whether by error message or by process timing." "A single error message **should** be employed and output the same way for each type of decryption error. There **should** be no difference in the observable behavior for the different RSA-OAEP decryption errors." "care should be taken to ensure that even if there are no errors, an implementation does not reveal partial information about the encoded message EM" "the observable behavior of the mask generation function **should not** reveal even partial information about the MGF seed employed in the process"	Yes	N/A
7.2.3 RSA-based Key-Encapsulation Mechanism with a Key-Wrapping Scheme (RSA-KEM-KWS)	N/A, no shall statements	"Care **should** be taken to ensure that the different error conditions in Steps 2.2, 4, and 6 cannot be distinguished from one another by an opponent, whether by error message or timing." "A single error message	Yes	N/A

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
		should be employed and output the same way for each error type. There **should** be no difference in timing or other behavior for the different errors. In addition, care **should** be taken to ensure that even if there are no errors, an implementation does not reveal partial information about the shared secret Z.” “care **should** be taken to ensure that an implementation does not reveal information about the encapsulated secret value Z. For instance, the observable behavior of the KDF **should not** reveal even partial information about the Z value employed in the key derivation process.”		
8 Key Agreement Schemes	In many cases TLS is deployed only with server authentication.	None.	Yes	N/A
8.1 Common Components for Key Agreement	N/A, no shall statements	None.	Yes	N/A
8.2 The KAS1 Family	N/A, no shall statements	None.	Yes	N/A
8.2.1 KAS1 Family Prerequisites	None.	None.	Yes	N/A
8.2.2 KAS1-basic	None.	None.	Yes	N/A
8.2.3 KAS1 Key Confirmation	None.	None.	Yes	N/A
8.2.4 KAS1 Security Properties	N/A, no shall statements	None.	Yes	N/A
8.3 The KAS2 Family	N/A, no shall statements	None.	Yes	N/A

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
8.3.1 KAS2 Family Prerequisites	None.	None.	Yes	N/A
8.3.2 KAS2-basic	None.	"the observable behavior of the key-agreement process **should not** reveal partial information about the shared secret Z."	Yes	N/A
8.3.3 KAS2 Key Confirmation	None.	None.	Yes	N/A
8.3.4 KAS2 Security Properties	N/A, no shall statements	None.	Yes	N/A
9 IFC based Key Transport Schemes	None.	None.	Yes	N/A
9.1 Additional Input	None.	None.	Yes	N/A
9.2 KTS-OAEP Family: Key Transport Using RSA-OAEP	N/A, no shall statements	None.	Yes	N/A
9.2.1 KTS-OAEP Family Prerequisites	None.	None.	Yes	N/A
9.2.2 Common components	N/A, no shall statements	None.	Yes	N/A
9.2.3 KTS-OAEP-basic	None.	None.	Yes	N/A
9.2.4 KTS-OAEP Key Confirmation	None.	None.	Yes	N/A
9.2.5 KTS-OAEP Security Properties	N/A, no shall statements	None.	Yes	N/A
9.3 KTS-KEM-KWS Family: Key Transport using RSA-KEM-KWS	N/A, no shall statements	None.	Yes	N/A
9.3.1 KTS-KEM-KWS Family Prerequisites	None.	None.	Yes	N/A
9.3.2 Common Components of the	N/A, no shall statements	None.	Yes	N/A

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
KTS-KEM-KWS Schemes				
9.3.3 KTS-KEM-KWS-basic	None.	None.	Yes	N/A
9.3.4 KTS-KEM-KWS Key Confirmation	None.	None.	Yes	N/A
9.3.5 KTS-KEM-KWS Security Properties	N/A, no shall statements	None.	Yes	N/A

9 ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 28: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[NDPP]	U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) and Traffic Filter Firewall Extended Package (TFFWEP)
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-2]	FIPS PUB 186-2 Federal Information Processing Standards Publication 2000 January 27
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008