Cisco Intrusion Prevention System 7.2(1)

Security Target

Version 1.2

July, 2013

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
ASA	Cisco Adaptive Security Appliances
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
DSU	Data Service Unit
EAL	Evaluation Assurance Level
Gbps	Gigabit per second
GRE	Generic Routing Encapsulation
HTTPS	Hyper-Text Transport Protocol Secure
IDM	IPS Device Manager
IME	IPS Manager Express
IPS	Intrusion Prevention System
ISDN	Integrated Services Digital Network
IT	Information Technology
MPLS	Multiprotocol Label Switching
NDPP	Network Device Protection Profile
NME-IPS	Cisco IPS Network Module
OS	Operating System
PP	Protection Profile
SFP	Small–form-factor pluggable port
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SSC	Security Services Cards
SSM	Security Services Module
SSHv2	Secure Shell (version 2)
SSP	Security Services Processor
ST	Security Target
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VLAN	Virtual Local Area Network
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 Intrusion Prevention System (IPS). 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 Intrusion Prevention System 7.2(1)
ST Version	1.2
Publication Date	July, 2013
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Intrusion Prevention System
TOE Hardware Models	IPS 4300 and 4500 series sensors (4345, 4360, 4510, and 4520); IPS hardware modules for ASA 5585-X (IPS SSP-10, SSP-20, SSP-40, and SSP-60); IPS software modules on ASA 5500-X.
TOE Software Version	7.2(1)
ST Evaluation Status	In Evaluation
Keywords	Intrusion Prevention System, Data Protection, Authentication

1.2 TOE Overview

The Cisco Intrusion Prevention System TOE consists of both hardware and software solutions deployed as network appliances, and evaluated as generic network devices as defined by the Network Device Protection Profile (NDPP) v1.1. The TOE includes both software and hardware models as described in Table 2 in section 1.1.

1.2.1 TOE Product Type

The Cisco Intrusion Prevention System is a family of network-based intrusion detection and prevention appliances. These appliances offer range of specialized security functionality that is outside the logical scope of evaluation as defined by the NDPP. The specialized network traffic inspection and attack prevention functionality is outside the scope of evaluation, but does not interfere with the evaluated functionality, so any of the IPS functionality can remain enabled in the certified configurations.

As a network device, the TOE supports self-protection through implementation of authentication mechanisms for local and remote administration, and use of encrypted network protocols for remote administration. The TOE also supports generation of an array of security-relevant audit messages, and the ability to have those messages transmitted over encrypted network protocols to authenticated remote hosts.

The specialized IPS functionality that is outside the scope of evaluation, but which defines the product type includes the ability to monitors and react to network traffic in real-time, able to analyze the header and content of each packet. The Cisco IPS can analyze single packets or a complete flow for attacks while maintaining flow state, allowing for the detection of multi-packet attacks. The Cisco IPS uses a rule-based expert system to analyze the packet information to determine the type of attack, be it simple or complex.

All data collection and analysis is performed by the Cisco IPS which is to be placed at strategic points throughout a target IT network to collect and analyze passing network traffic. In response to an attack, the IPS has several options that include generating an alarm, logging the alarm event, dropping and modifying packets (e.g., defragmentation, TCP stream reassembly), sending a command to a Cisco router, switch, or firewall to block traffic specific offending network traffic, and killing Transfer Control Protocol (TCP) sessions.

Key features of the IPS product type that are outside the logical scope of evaluation include:

- Provides network-wide, distributed protection from many attacks, exploits, worms and viruses exploiting vulnerabilities in operating systems and applications.
- Provides Risk Rating based IPS policy provisioning, an authorized administrator assigns IPS policies based on risk, instead of tuning individual signatures. All events are assigned a Risk Rating number between 0 and 100 based on the risk level of the event. Based on the Risk Rating, different policy actions can be assigned, including drop packet, alarm, and log.
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions. No traffic can continue through the TOE without first passing through, and being inspected by the TOE. Note: IPS 4300 and 4500 sensors can be installed inline (such that network traffic flows through them) to provide this

functionality independent of another traffic filtering device such as a firewall or router. IPS SSP modules (hardware or software) support inline traffic inspection by working in consort with their host ASA firewall.

- Offers promiscuous mode inspection. In this mode a duplicate stream of traffic is sent to the TOE. Unlike operation in inline mode, the TOE operating in promiscuous mode can only block traffic by instructing the router/switch appliance to shun the traffic or by resetting a connection on the switch/router.
- Supports more than 3700 signatures from the same signature database available for Cisco IPS.
- Cisco anomaly detection provides powerful protection against day-zero attacks. The TOE learns the normal behavior on the network and creates an alert when it sees anomalous activities in the network. This provides protection against new threats even before signatures are available.
- Identifies the source of and blocks denial of service (DoS), distributed denial of service (DDoS), SYN flood, and encrypted attacks with Cisco Global Correlation.
- Uses patented anti-evasion technology to defend and monitor against worms, viruses, Trojans, reconnaissance attacks, spyware, botnets, phishing, peer to peer attacks, and malware, as well as numerous evasion techniques.

1.2.2 TOE Components

The descriptions of the Cisco IPS models below is provided to highlight key distinctions between the models, however these distinctions are not security-relevant with respect to the security requirements of the NDPP.

1.2.2.1 Cisco IPS 4300 and 4500 Sensors

The Cisco IPS 4300 and 4500 Sensors are standalone IPS appliances that provide hardware-accelerated deep packet inspection and automated threat management. Deep packet inspection can be done on encapsulated traffic, including generic routing encapsulation (GRE), Multiprotocol Label Switching (MPLS), 802.1q, IPv4 in IPv4, IPv4 in IPv6, and Q-in-Q double VLAN.

1.2.2.2 Cisco IPS SSP Hardware Modules

The IPS SSP hardware modules install to ASA 5500-X series firewalls. The host ASA provides power and cooling for the hardware module, but the hardware module provides its own physical management port. The IPS hardware module runs its own IPS operating system independent of the ASA operating system, with its own set of administrative users, its own audit configurations, etc. Administrators of the ASA cannot authenticate to the IPS and thus cannot modify the configuration of the IPS.

1.2.2.3 Cisco IPS SSP Software Modules

The IPS SSP software modules function just like the IPS hardware modules except they rely on the host ASA to provide physical interfaces for local and remote administration of the IPS. The IPS SSP software module and the ASA share the network-based Management interface (used for remote access, and audit log transmission); however, the IPS SSP and ASA each has its own separate MAC addresses and IP addresses. The IPS administrator configures the IP address of the IPS management interface within the IPS operating system, though physical characteristics (such as enabling the interface) on performed in the ASA operating system by the ASA administrator. The IPS SSP software modules can be installed to ASA in any of the ASA 5500-X models.

1.2.2.4 Cisco IPS Device Manager (IDM)

Cisco IDM is a Web-based tool/applet for sensor configuration and management. It can be accessed through Internet Explorer, Netscape, or Mozilla, by using the browser to connect to the IPS management interface, and when downloaded initiates its own Transport Layer Security (TLS) connection to the IPS for remote administration.

1.2.3 Non-TOE Components

1.2.3.1 Cisco ASA 5585-X

The Cisco ASA 5585-X is a high-performance, 2-slot chassis, with the firewall/VPN Security Services Processor (SSP) occupying the bottom slot, and the IPS Security Services Processor (IPS SSP) in the top slot of the chassis. The firewall/VPN SSP is required to run IPS on the Cisco ASA 5585-X. The IPS software runs on the IPS SSP hardware module. The Cisco ASA 5585-X Security Appliances scale from the Cisco Borderless Network Architecture to data center architectures, with integrated form factors ranging from 4 Gbps to 40 Gbps.

1.2.3.2 Cisco ASA 5500-X

The Cisco ASA 5500-X Series midrange security appliances include ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. The Cisco ASA 5500-X Series appliances provide additional network security through optional integrated cloud- and software-based security services that use identity for security policy selection, requiring no additional hardware modules. The Cisco ASA 5500-X appliances scale from the Cisco Borderless Network Architecture to data center architectures, with integrated form factors ranging from 1 Gbps to 4 Gbps.

1.2.3.3 Cisco IPS Manager Express (IME)

The IME is a powerful all-in-one IPS management application designed to meet the needs of small and medium-sized businesses. IME is a network management application that provides system health, events, and collaboration monitoring in addition to reporting and configuration for up to ten sensors. IME monitors sensor health using customizable dashboards and provides security alerts through RSS feed integration from Cisco Security Center. It monitors global correlation data, which an authorized administrator can view in events and reports. It monitors events and lets an authorized administrator sort views by filtering, grouping, and colorization. IME can embed the IPS Device Manager (IDM) configuration component to allow for a seamless integration between the monitoring and configuration of IPS devices.

1.2.3.4 Cisco Security Manager 4.x

Cisco Security Manager is an enterprise-class security management software application. It can be used to manage security policies on a wide variety of devices, including adaptive security appliances (ASA), intrusion prevention system (IPS) appliances and service modules, integrated security routers (ISRs), and so forth. An authorized administrator can also use Security Manager to view events generated from ASA and IPS devices.

Cisco Security Manager 4.x offers:

- Flexible processes to provision new and updated signatures incrementally, create IPS policies for those signatures, and then share the policies across devices
- Integrated tuning and troubleshooting tools including IPS event-to-policy linkages and cross-launching capabilities
- Enhanced reporting and event management support for Cisco’s latest IPS features, including Global Correlation
- Role-based access control and workflow, which help ensure error-free deployments and process compliance

1.2.4 Supported non-TOE Hardware/ Software/ Firmware

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

Table 3: Operational Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client and/or TLS client	Yes	This includes any management workstation with a SSH client supporting SSHv2, or TLS/HTTPS client (web browser) supporting TLSv1.2. These clients are used for remote administration of the TOE.
Audit Retrieval Software/Server	Yes	Audit retrieval software such as Cisco IPS Manager Express (IME) capable of initiating TLS/HTTPS connection to the TOE to retrieve audit log files.
NTP Server	No	The TOE supports communications with an NTP server for clock updates.
WIC	No	WICs (wide-area-network interface cards) provide the network interfaces used by port adaptors to communicate on wide area networks (WANs). Any Cisco WIC is supported. Examples include, Ethernet High-Speed WICs, Wireless High-Speed WICs, Serial WICs, CSU/DSU WICs, and ISDN BRI WICs.
ASA 5500-X	For IPS Software Module	Any of 5512-X, 5515-X, 5525-X, 5545-X, or 5555-X running ASA 8.6(1) or later is required to support the IPS software module.
ASA 5585-X	For IPS Hardware Module	ASA 5585-X running ASA 8.4(2) is required to the support the IPS hardware modules IPS SSP-10, SSP-20, SSP-40, or SSP-60.
Any ASA	For IPS 4300/4500	When an IPS 4300 or 4500 is not installed in-line (with traffic flowing through the IPS appliance), the IPS sensor works in tandem with an ASA to facilitate blocking of traffic. Compatible ASA models include 5505, 5510, 5520, 55040, 5550, 5580, 5500-X, and 5585-X.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Intrusion Prevention System Target of Evaluation (TOE). The TOE configurations include both software and hardware. The hardware is comprised of the following: IPS 4300 and 4500 Series Sensors; and ASA 5585-X SSP hardware modules. The software is comprised of the IPS software image Release 7.2(1).

The following figure provides a visual depiction of an example TOE deployment.

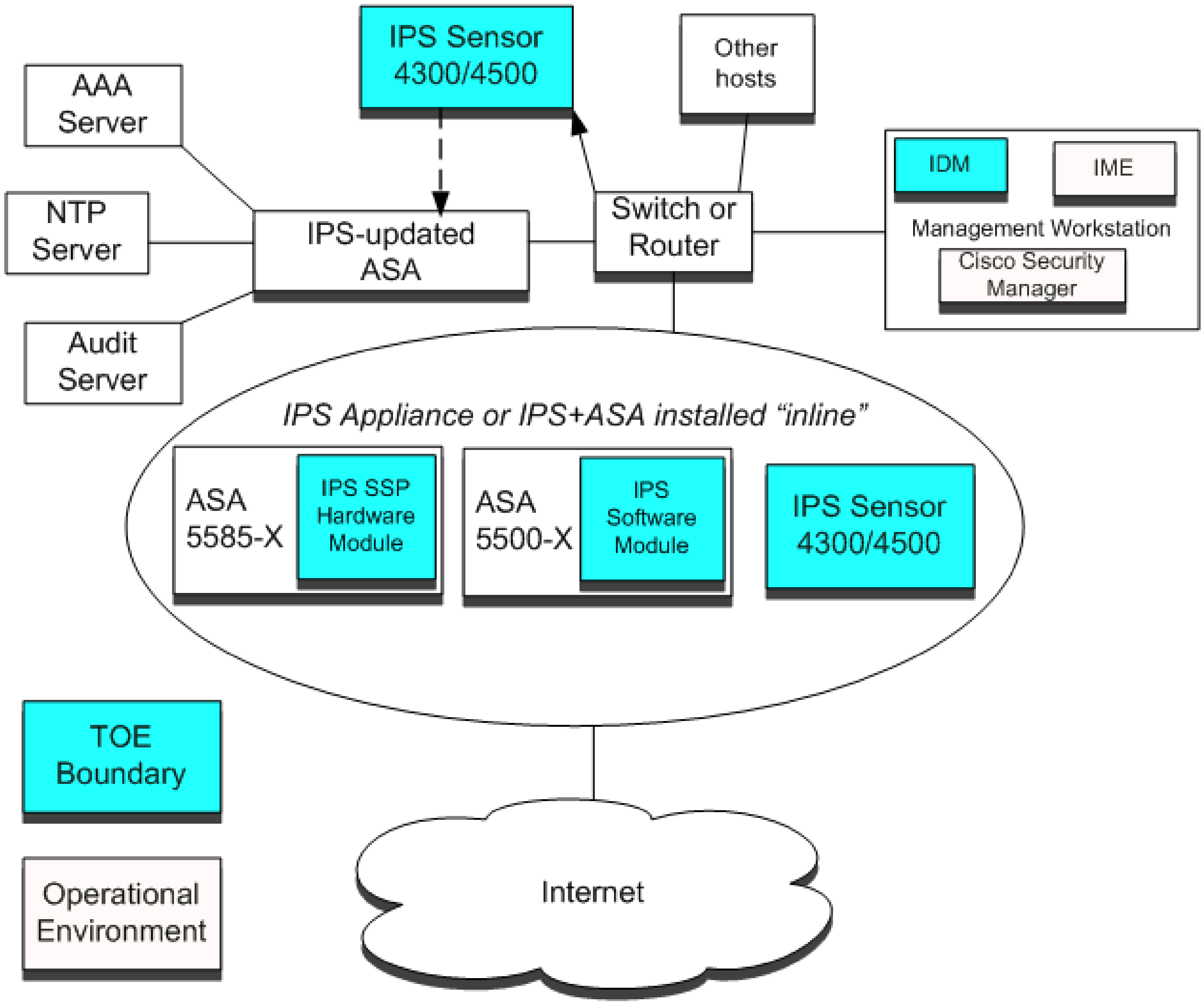


Figure 1 Example TOE Deployment

The figure above includes the following:

- Several examples of TOE Hardware Modules and Sensors
  - IPS Sensor appliance
  - IPS SSP hardware module (on ASA 5585-X, which is outside the TOE boundary)
  - IPS SSP software module (on ASA 5500-X, which is outside the TOE boundary)
  - IDM (on a management workstation, which is outside the TOE boundary)
- Operational Environment Components:
  - Management Workstation (with IDM or CSM, and an SSH client)
  - AAA Server
  - NTP Server
  - Audit retrieval/storage application such as IME

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 IPS software.

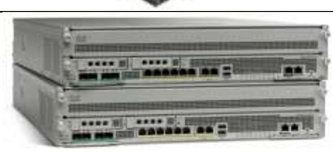
In the evaluated configurations, the TOE:

- Must have an audit file retrieval server must be provided to connect to the IPS over TLS/HTTPS to retrieve and store audit records;
- Can be remotely administered accessing its CLI via SSHv2;
- Can be remotely administered accessing its GUI (IDM) via TLS/HTTPS;
- Can connect to an NTP server for clock updates.

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution. The TOE hardware includes the following models: IPS 4300 and 4500 Series Sensors, ASA 5585-X SSP hardware module. The software is comprised of the IPS software image Release 7.2(1). The network, on which they reside, is considered part of the environment. The TOE is comprised of the following specifications as described in Table 4 below:

Table 4: TOE Specifications

Hardware/Software	Picture	Size (H x W X D)	Interfaces
Cisco IPS 4345 Sensor		1.67 x 16.9 x 15.5 in.	(1) Ethernet 10/100 port
Cisco IPS 4360 Sensor		1.67 x 16.7 x 19.1 in.	(1) Ethernet 10/100 port
Cisco IPS 4510 Sensors		3.47 x 19 x 26.5 in.	(6) port 10/100/1000, (4) port 1 or 10 Gigabit Ethernet SFP+
Cisco IPS 4520 Sensor		3.47 x 19 x 26.5 in.	(6) port 10/100/1000, (4) port 1 or 10 Gigabit Ethernet SFP+
Cisco ASA 5512-X IPS Note: This is a software-only IPS product.	IPS software runs on ASA 5500-X series firewalls: 	N/A	Virtual management and network interfaces
Cisco ASA 5515-X IPS Note: This is a software-only IPS product.		N/A	Virtual management and network interfaces
Cisco ASA 5525-X IPS Note: This is a software-only IPS product.		N/A	Virtual management and network interfaces
Cisco ASA 5545-X IPS Note: This is a software-only IPS product.		N/A	Virtual management and network interfaces

Hardware/Software	Picture	Size (H x W X D)	Interfaces
Cisco ASA 5555-X IPS Note: This is a software-only IPS product.		N/A	Virtual management and network interfaces
Cisco ASA 5585-X SSP-10	SSP runs on the ASA 5585-Xfirewalls: 	1.70 x 17.20 x 15.60 in. (4.32 x 43.69 x 39.62 cm)	Physical management interface, plus virtual network interfaces
Cisco ASA 5585-X SSP-20		1.70 x 17.20 x 15.60 in. (4.32 x 43.69 x 39.62 cm)	Physical management interface, plus virtual network interfaces
Cisco ASA 5585-X SSP-40		1.70 x 17.20 x 15.60 in. (4.32 x 43.69 x 39.62 cm)	Physical management interface, plus virtual network interfaces
Cisco ASA 5585-X SSP-60		1.70 x 17.20 x 15.60 in. (4.32 x 43.69 x 39.62 cm)	Physical management interface, plus virtual network interfaces

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. Protection of the TSF
7. TOE access
8. Trusted path/channels

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

1.6.1 Security audit

The Cisco Intrusion Prevention System provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco IPS routers generate an audit record for each auditable event. The administrator configures auditable events, backs-up, and manages audit data storage. The TOE provides the audit trail protection by providing remote backup to a syslog server.

1.6.2 Cryptographic support

The TOE provides cryptography in support of other Cisco IPS security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 2. The TOE provides cryptography in support of remote administrative management via SSHv2 and TLSv1.0, TLSv1.1, and TLSv1.2. The cryptographic services provided by the TOE are described in Table 5 below.

Table 5: TOE Provided Cryptography

Cryptographic Method	Use within the TOE
RSA Signature Services	Used in SSH session establishment.
SP 800-90 RBG	Used in SSH session establishment.
SHS	Used to provide traffic integrity verification for SSH and TLS.
AES	Used to encrypt session traffic for SSH and TLS.

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 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 provides authentication of administrators to use a local user database, supporting password-based authentication at either the serial console, or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys.

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 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; and TOE configuration file storage and retrieval. All of the security relevant management functionality described in the paragraph above can only be performed by an authorized administrator.

Administrators can create configurable login banners to be displayed at time of login, and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

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. Additionally Cisco IPS is not a general-purpose operating system and access to Cisco IPS functionality is restricted to only Cisco IPS processes and IPS administrators.

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. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

1.6.7 TOE Access

The TOE can terminate inactive sessions after an authorized administrator configurable time-period. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an authorized administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

1.6.8 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 and TLSv1.2. When configured by an Administrator to dynamically modify access control lists on compatible network traffic filtering devices such as routers and firewalls, the TOE supports initiation of SSH connections to those network devices. The TOE also supports remote retrieval of audit records over TLS/HTTPS connections initiated to the TOE from authorized and authenticated remote systems.

1.7 Excluded Functionality

The following functionality is excluded from use in the certified configurations.

Table 6: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Use of telnet for remote administration.	The NDPPv1.1 requires all remote administration to be secured in one of IPsec, SSH, or TLS. Use of telnet would transmit authentication and configuration data unencrypted. SSHv2 will be used for remote administration via the CLI.
Use of HTTP (instead of HTTPS/TLS) for remote administration or for retrieval of event log data.	The NDPPv1.1 requires all remote administration to be secured in one of IPsec, SSH, or TLS. Use of HTTP would transmit authentication and configuration data unencrypted. TLS will be used for remote administration via any GUI, and for retrieval of event log data.

Excluded Functionality	Exclusion Rationale
Use of RADIUS and TACACS+	The NDPPv1.1 requires all communications with remote AAA servers to be tunneled in one of IPsec, SSH, or TLS. The Cisco IPS does not support tunneling, so remote AAA servers cannot be used in the certified configuration.
Use of some TLS ciphersuites including: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	The NDPPv1.1 defines a list of TLS ciphersuites that are either 'mandatory' or 'optional' in a certified configuration. The Cisco IPS supports all of the mandatory ciphersuites, and some of the optional ciphersuites, but the configuration option in the Cisco IPS that would enable the supported optional ciphersuites would result in enabling other ciphersuites that are not allowed by the NDPP.

This functionality 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. All other functionality supported in the Cisco IPS product can be used in the evaluated configuration without interfering with the evaluated functionality of the TOE.

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.

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 U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP).

This ST claims compliance to the following Common Criteria validated Protection Profiles:

Table 7: Protection Profiles

Protection Profile	Version	Date
U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP)	1.1	June 8, 2012

2.2.1 Protection Profile Refinements

None.

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 Profile:

- U.S. Government Protection Profile for Security Requirements for Network Devices

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 NDPP 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 NDPP 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 NDPP for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this 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.

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 8: 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.

3.2 Threats

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

Table 9: Threats

Threat	Threat Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
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.
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.

3.3 Organizational Security Policies

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

Table 10: 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 Operational 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 11: Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
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.

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 12: Security Objectives for the Environment

Environment Security Objective	Operational Environment Security Objective Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
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.

4.3 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.

4.3.1 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 13: Tracing of security objectives to SPD

	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.ADMIN_ERROR	T.UNDETECTED_ACTIONS	T.RESOURCE_EXHAUSTION	T.USER_DATA_REUSE	T.TSF_FAILURE	T.TRANSMIT	P.ACCESS BANNER
O.PROTECTED_COMMUNICATIONS											X	
O.VERIFIABLE_UPDATES					X							
O.SYSTEM_MONITORING							X					
O.DISPLAY_BANNER												X
O.TOE_ADMINISTRATION						X						
O.RESIDUAL_INFORMATION_CLEARING									X			

	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.ADMIN_ERROR	T.UNDETECTED_ACTIONS	T.RESOURCE_EXHAUSTION	T.USER_DATA_REUSE	T.TSF_FAILURE	T.TRANSMIT	P.ACCESS BANNER
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									

4.3.2 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.

4.3.2.1 Tracing of assumptions

Table 14: Assumption 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

4.3.2.2 Tracing of threats and OSPs

Table 15: 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.

4.3.3 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.

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:

- Where operations were completed in the NDPP itself, the formatting used in the NDPP has been retained;
- Assignment: Indicated with *italicized* text, which may or may not be bracketed;
- Refinement made by PP author: Indicated with **bold** text; may have **Refinement:** at the beginning of the element for further clarification.
- Selection: Indicated with <u>underlined</u> text, which may or may not be bracketed;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

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 16: Security Functional Requirements

Class Name	Component Identification	Component Name
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices		
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	HTTPS

Class Name	Component Identification	Component Name
	FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
	FCS_SSH_EXT.1	SSH
	FCS_TLS_EXT.1	TLS
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 7TSF 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	Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_STM.1	Reliable Time Stamps
	FPT_TUD_EXT.1	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

5.2.1 Security audit (FAU)

5.2.1.1 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 17].

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 17].

Table 17 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
Security Functional Requirements Drawn from NDPP		
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.
FC_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_RBG_EXT.1	None.	
FCS_TLS_EXT.1	Failure to establish a TLS session. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
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_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 by	No additional information.

SFR	Auditable Event	Additional Audit Record Contents
	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.

5.2.1.2 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.

5.2.1.3 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 TLS/HTTPS protocol.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 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 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard")*
- *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.

5.2.2.2 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.

5.2.2.3 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 mode***]] and cryptographic key sizes 128-bits, 256-bits, and <u>no other key sizes</u> that meets the following:

- **F**IPS **PUB 197, "Advanced Encryption Standard (AES)"**
- **<u>NIST SP 800-38A</u>**

5.2.2.4 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:
<u>RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater,</u>

that meets the following:

Case: RSA Digital Signature Algorithm

- **F**IPS **PUB 186-2 or F**IPS **PUB 186-3, "Digital Signature Standard"**

5.2.2.5 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 **<u>SHA-1</u> and message digest sizes <u>160</u> bits** that meet the following: *F*IPS *Pub 180-3, "Secure Hash Standard."*

5.2.2.6 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-**<u>[SHA-1</u>], key size [*160-bits*]**, **and message digest sizes [160] bits** that meet the following: [*F*IPS *Pub 198-1, "The Keyed-Hash Message Authentication Code, and F*IPS *Pub 180-3, "Secure Hash Standard."*]

5.2.2.7 FCS_HTTPS_EXT.1 Explicit: HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

5.2.2.8 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 NIST Special Publication 800-90 using CTR_DRBG (AES) seeded by an entropy source that accumulated entropy from a software-based noise source..

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of 256 bits of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

5.2.2.9 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 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.

5.2.2.10 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) TLS 1.1 (RFC 4346), and TLS 1.2 (RFC 5246)] 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

5.2.3 User data protection (FDP)

5.2.3.1 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.

5.2.4 Identification and authentication (FIA)

5.2.4.1 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: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “[“, *“+”, “:”, “,”, “_” (underscore), “/”, “-“, “?”, and “]”*;
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

5.2.4.2 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;
- *no other actions*.

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.

5.2.4.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, *and a local public key-based authentication mechanism consistent with FCS_SSH_EXT.1.2* to perform administrative user authentication.

5.2.4.4 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.

5.2.5 Security management (FMT)

5.2.5.1 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*.

5.2.5.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 Refinement: 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 list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*
- *Ability to configure the cryptographic functionality*]

5.2.5.3 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.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 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.

5.2.6.2 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.

5.2.6.3 FPT_STM.1 Reliable time stamps

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

5.2.6.4 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 <u>published hash</u> prior to installing those updates.

5.2.6.5 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.

5.2.6.6 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

- <u>terminate the session</u>]

after a Security Administrator-specified time period of inactivity.

5.2.6.7 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*].

5.2.6.8 FTA_SSL.4 User-initiated Termination

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

5.2.6.9 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.

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall **use [<u>SSH, TLS/HTTPS</u>]** to provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [*<u>remote traffic-filtering devices, remote audit servers, remote iplog storage hosts, remote file servers</u>*]** 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 [*communications with the following:*

- *remote traffic-filtering devices over SSH*
- *remote audit servers over TLS/HTTPS*
- *remote iplog storage hosts over SCP (SSH) or TLS/HTTPS*
- *remote file servers containing software/firmware updates over SCP (SSH) or TLS/HTTPS*].

5.2.7.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 Refinement: The TSF shall **use** [**SSH, 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*.

5.3 Rationale for Explicitly Stated Requirements

Table 18: Rationale for Explicitly Stated Requirements

SFR	Rationale
FAU_STG_EXT.1	Drawn from NDPP v1.1.
FCS_CKM_EXT.4	Drawn from NDPP v1.1.
FCS_HTTPS_EXT.1	Drawn from NDPP v1.1.
FCS_RBG_EXT.1	Drawn from NDPP v1.1.
FCS_SSH_EXT.1	Drawn from NDPP v1.1.
FCS_TLS_EXT.1	Drawn from NDPP v1.1.
FIA_PMG_EXT.1	Drawn from NDPP v1.1.
FIA_UIA_EXT.1	Drawn from NDPP v1.1.
FIA_UAU_EXT.2	Drawn from NDPP v1.1.
FPT_SKP_EXT.1	Drawn from NDPP v1.1.
FPT_APW_EXT.1	Drawn from NDPP v1.1.
FPT_TST_EXT.1	Drawn from NDPP v1.1.
FPT_TUD_EXT.1	Drawn from NDPP v1.1.
FTA_SSL_EXT.1	Drawn from NDPP v1.1.

5.4 SFR Dependencies Rationale

Functional component FCS_COP.1 depends on the following functional components: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction and FMT_MSA.2 Secure Security Attributes. Cryptographic modules must be FIPS PUB 140-2 compliant. If the cryptographic module is indeed compliant with this FIPS PUB, then the dependencies of key generation, key destruction and secure key values will have been satisfied in becoming FIPS PUB 140-2 compliant. For more information, refer to section 4.7 of FIPS PUB 140-2.

Table 19: SFR Dependency Rationale

SFR	Dependency	Rationale
Security Functional Requirements Drawn from NDPP		
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Met by FAU_GEN. Met by FIA_UID.2
FAU_STG_EXT.1	FAU_GEN.1	Met by FAU_GEN.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], and FCS_CKM.4	Met by FCS_COP.1(2) Met by FCS_CKM_EXT.4
FCS_CKM_EXT.4	FDP_ITC.1 or 2 or FCS_CKM.1	Met by FCS_CKM.1(1)
FCS_COP.1(1)	[FDP_ITC.1 or 2 or FCS_CKM.1], and FCS_CKM.4	Met by FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(2)	[FDP_ITC.1 or 2 or FCS_CKM.1], and FCS_CKM.4	Met by FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(3)	[FDP_ITC.1 or 2 or FCS_CKM.1], and FCS_CKM.4	Met by FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(4)	[FDP_ITC.1 or 2 or FCS_CKM.1], and FCS_CKM.4	Met by FCS_CKM.1 and FCS_CKM_EXT.4
FCS_HTTPS_EXT.1	FCS_TLS.1	Met by FCS_TLS.1
FCS_RBG_EXT.1	FCS_CKM.1	Met by FCS_CKM.1
FCS_SSH_EXT.1	FCS_COP.1	Met by FCS_COP.1
FCS_TLS_EXT.1	FCS_COP.1	Met by FCS_COP.1
FDP_RIP.2	No dependencies	Not Applicable
FIA_PMG_EXT.1	FIA_UAU_EXT.2	Met by FIA_UAU_EXT.2
FIA_UIA_EXT.1	FTA_TAB.1	Met by FTA_TAB.1
FIA_UAU_EXT.2	FIA_UIA_EXT.1	Met by FIA_UIA_EXT.1
FIA_UAU.7	FIA_UIA_EXT.1	Met by FIA_UIA_EXT.1

SFR	Dependency	Rationale
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Met by FMT_SMF.1 Met by FMT_SMR.1
FMT_SMF.1	No dependencies	Not Applicable
FMT_SMR.1	FIA_UID.1	Met by FIA_UIA_EXT.1 since FIA_UIA_EXT.1 meets the requirements of FIA_UID.2 which is hierarchical to FIA_UID.1.
FPT_SKP_EXT.1	FCS_CKM.1	Met by FCS_CKM.1
FPT_APW_EXT.1	FIA_PMG_EXT.1.1	Met by FIA_PMG_EXT.1.1
FPT_STM.1	No dependencies	Not Applicable
FPT_TST_EXT.1	No dependencies	Not Applicable
FPT_TUD_EXT.1	FCS_COP.1(2) FCS_COP.1(3)	Met by FCS_COP.1(2) FCS_COP.1(3)
FTA_SSL_EXT.1	FIA_UAU.1	Met by FIA_UIA_EXT.1 since FIA_UIA_EXT.1 meets the requirements of FIA_UAU.1.
FTA_SSL.3	No dependencies	Not Applicable
FTA_SSL.4	No dependencies	Not Applicable
FTA_TAB.1	No dependencies	Not Applicable
FTP_ITC.1	No dependencies	Not Applicable
FTP_TRP.1	No dependencies	Not Applicable

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

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

Table 20: 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

5.5.2 Security Assurance Requirements Rationale

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.

5.5.3 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 21: Assurance Measures

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

Component	How requirement will be met
ALC_CMS.1	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.
ATE_IND.1	Cisco provides the TOE for independent testing.
AVA_VAN.1	Cisco provides the TOE for vulnerability analysis.

6 TOE SUMMARY SPECIFICATION

6.1 Security Requirements Rationale

Table 22: Security Requirements Mapping to Objectives

	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
FAU_GEN.1			X		X				
FAU_GEN.2			X						
FAU_STG_EXT.1	X		X		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.1	X								
FCS_RBG_EXT.1	X								
FCS_SSH_EXT.1	X								
FCS_TLS_EXT.1	X								
FDP_RIP.2						X			
FIA_PMG_EXT.1					X				
FIA_UIA_EXT.1					X				
FIA_UAU_EXT.2					X				
FIA_UAU.7					X				
FMT_MTD.1					X				

	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
FMT_SMF.1					X				
FMT_SMR.2					X				
FPT_ITT.1	X								
FPT_SKP_EXT.1	X								
FPT_APW_EXT.1					X				
FPT_STM.1			X		X				
FPT_TUD_EXT.1		X							
FPT_TST_EXT.1									X
FTA_SSL_EXT.1					X			X	
FTA_SSL.3					X			X	
FTA_SSL.4					X			X	
FTA_TAB.1				X					
FTP_ITC.1	X								
FTP_TRP.1	X								

6.2 TOE Security Functional Requirement Measures

Table 23 identifies and describes how the Security Functional Requirements identified in section 5 of this ST are met by the TOE.

Table 23: How the SFRs Are Satisfied

TOE SFRs	How the SFR is Satisfied
Security Functional Requirements Drawn from NDPP	
FAU_GEN.1	The TOE is able to generate audit records that are stored internally within the TOE whenever an audited event occurs. The types of events that cause audit records to be generated include: startup of the audit mechanism, cryptography related events including use of secure network protocols; identification and authentication related events; and administrative actions. Each of the messages contains sufficient detail to identify the user for which the event is associated, when the event occurred, where

TOE SFRs	How the SFR is Satisfied
	the event occurred, the outcome of the event, and the type of event that occurred. Auditable events related to failure to establish secure sessions include: • SSH client: failures to negotiate SSH version, or session parameters including cipher, hmac, or dh group. • SSH server: login failures including: invalid user, or invalid password/key; or failure to negotiate SSH version; or failures to negotiate parameters including cipher, hmac, or dh group. • TLS/HTTPS server: authentication failures including: invalid user, invalid password, or invalid certificate.
FAU_GEN.2	The TOE shall ensure that each auditable event is associated with the username that triggered the event and as a result they are traceable to a specific user. For example a human user, user identity, or related session ID would be included in the audit record. For an IT entity or device, the IP address, or other configured identification is presented. Refer to the Guidance documentation for configuration syntax and information.
FAU_STG_EXT.1	The TOE is configured to allow audit logs to be retrieved by a remote audit server. The TOE protects communications with an external audit server via TLS/HTTPS. The TOE stores audit records locally on the TOE, and continues to do so after audit logs are retrieved (pulled) by a remote audit server. The local event store holds a maximum of 30MB (on all platforms). When event store is full, the oldest events will be overwritten by new events. Only authorized administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.
FCS_CKM.1	The TOE implements a random number generator for Diffie-Hellman key establishment (conformant to NIST SP 800-56A), and for RSA key establishment schemes (conformant to NIST SP 800-56B). Refer to Annex A of this document for more detailed compliance information relative to NIST SP 800-56. The TOE can create a RSA public-private key pair and generate a self-signed certificate, and functions as its own Certificate Authority (CA).
FCS_CKM_EXT.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) in that none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext form. Further zeroization details are provided in Annex A of this document. (FIPS #1668)
FCS_COP.1(1)	The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128, 256 bits) as described in NIST SP 800-38A. (FIPS #1668 and #1758)
FCS_COP.1(2)	The TOE will provide cryptographic signature services using RSA with key size of 2048 and greater as specified in FIPS PUB 186-3, "Digital Signature Standard" and FIPS PUB 186-2, "Digital Signature Standard". (FIPS #1668 and #876)
FCS_COP.1(3)	The TOE provides cryptographic hashing services using SHA-1 as specified in FIPS Pub 180-3 "Secure Hash Standard." (FIPS #1668 and #1544)
FCS_COP.1(4)	The TOE provides keyed-hashing message authentication services using HMAC-SHA-1 as specified in FIPS Pub 198-1,"The Keyed-Hash Message Authentication Code," and FIPS 180-3, "Secure Hash Standard." (FIPS #1668 and #1031)
FCS_HTTPS_EXT.1	The TOE implements HTTPS conformant to RFC 2818. HTTPS is essentially

TOE SFRs	How the SFR is Satisfied
	HTTP layered on TLS or SSL (though only TLS is used in the TOE). HTTP version 1.1 (“HTTP/1.1", RFC 2616, as referenced in RFC 2818) is used to for the exchange of OSI application layer data between the client and server including username and password authentication credentials. TLS operates at a lower sub-layer of the OSI application layer, and after the TCP handshake has completed, TLS negotiates its own TLS handshake to negotiate cryptographic parameters for the secure transmission of HTTP(S). For further description of TLS, see the description of FCS_TLS_EXT.1 elsewhere in this table.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90. (FIPS #1668 and #937) The boundary of the entropy source is the entire TOE platform. An adversary on the outside is not able to affect the entropy rate in any determinable way, because of the number of sources, and the fact that the only one of the sources (allocated packet buffer) is populated with data that came from outside of the system.
FCS_SSH_EXT.1	The TOE implements SSHv2 (telnet is disabled in the evaluated configuration). SSH connections will be dropped if the TOE receives a packet larger than 65,535 bytes. • The TOE implementation of SSHv2 supports the following public key algorithms for authentication: RSA Signature Verification. • The TOE also supports local password-based authentication for administrative users accessing the TOE through SSHv2, and optionally supports deferring authentication to a remote AAA server. • The TOE implementation of SSHv2 supports the following encryption algorithms, AES-CBC-128, AES-CBC-256 to ensure confidentiality of the session. • The TOE’s implementation of SSHv2 supports hashing algorithm HMAC-SHA1to ensure the integrity of the session.
FCS_TLS_EXT.1	The TOE implements TLSv1.0 conformant to RFC 2246, TLS 1.1 conformant to RFC 4346, and TLS 1.2 conformant to RFC 5246. The TOE uses TLS/HTTPS to secure communications from remote administration workstations running IDM, CSM, or IME. Remote administrators can connect to the using TLS/HTTPS to download audit files. The TOE can initiate outbound TLS/HTTPS connections to download IPS signature file updates. The TOE can be configured to negotiate only the following four SHA-1 ciphersuites (defined as ‘mandatory’ by the NDPPv1.1): 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
FDP_RIP.2	The TOE ensures that packets transmitted from the TOE do not contain residual information from previous packets. Frames that are not at least the minimum length are padded with zeros. Residual data is never transmitted from the TOE because memory buffers are overwritten upon reuse. This applies to both data plane traffic and administrative session traffic. FDP_RIP.2 is enforced for sessions that terminate at the TOE, but also applies to traffic traversing the TOE (applicable to the IPS standalone appliances that support inline deployment).
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 that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “[“, “+”, “:”, “,”, “_” (underscore), “/”, “-“, “?”, and “]”. Minimum

TOE SFRs	How the SFR is Satisfied
	password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 8 to 64 characters.
FIA_UIA_EXT.1	The TOE requires all administrators 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 (via console or SSHv2), and/or through a remote GUI client such as IDM, CSM, or IME (all using TLS/HTTPS). The TOE mediates all administrative actions through the CLI and GUI. Once a potential administrative user attempts to access the TOE through either a directly connected console or remotely through an SSHv2 or TLS/HTTPS connection, 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 support for local public key-based authentication consistent with FCS_SSH_EXT.1.2 using RSA keys for SSH. The administrator authentication policies include authentication to the local user database which must be populated with passwords, and supports being augmented with RSA keys for account authentication when using SSH. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console or remotely via SSHv2 or TLS/HTTPS. At initial login the administrative user must provide a valid username with valid authentication credentials. The TOE then either grants administrative access (if the combination of username and credentials is valid) or indicates that the login was unsuccessful. The TOE does not provide the unauthenticated end-user with the reason for login failure (such as wrong password or invalid username).
FIA_UAU.7	When a user enters their password at the local console, via SSHv2, or via TLS/HTTPS, the TOE does not echo any characters of the password or any representation of the characters. This also prevents the number of characters in the password from being gleaned by an onlooker.
FMT_MTD.1	The TOE provides the ability for authorized administrators to access TOE data, such as audit data, configuration data, security attributes, IPS policies, routing tables, cryptographic settings, etc. Each of the predefined administrative roles has a set of permissions that grant users assigned to the role some level of access to the TOE data. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the appropriate privileges for their assigned role.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. Guidance documentation provides instruction for use of each administrative interface, including proper syntax, commands, and additional information about administrative functions.
FMT_SMR.2	The Network Device Protection Profile only allows for defining one administrative "role" for the purposes of evaluation. Cisco IPS provides more than one administrative role, so in this Security Target the term "authorized administrator" is used in this ST to refer to any authenticated (logged in) account assigned to any role. There are four administrative roles (only three of which are permitted to be used in the evaluated configuration): 1. Viewer: Can view configuration and events, but cannot modify any

TOE SFRs	How the SFR is Satisfied
	configuration data except their user passwords. 2. Operator: Can view everything and can modify the following options: a. Signature tuning (priority, disable or enable) b. Virtual sensor definition c. Managed routers d. Their user passwords 3. Administrator: Can view everything and can modify all options that Operators can modify in addition to the following: a. Sensor addressing configuration b. List of hosts allowed to connect as configuration or viewing agents c. Assignment of physical sensing interfaces d. Enable or disable control of physical interfaces e. Add and delete users and passwords f. Generate new SSH host keys and server certificates 4. Service: The service account must not be used in the evaluated configuration. Only a user with administrator privileges can create, edit, or delete the service account, 5. The service account is disabled by default, only one such account exists, and no others can be created. 6. If the service account is enabled, the TOE will no longer be in its evaluated configuration. The service account is a special account that does not use the standard IPS CLI shell, and is intended for troubleshooting purposes only by Cisco personnel. The service account would log into a bash shell rather than the standard IPS CLI shell. The service account cannot login to the IPS sensor via IDM, CSM, or IME.
FPT_SKP_EXT.1	The TOE stores all private keys not readily accessible to administrators. All pre-shared, symmetric, and private keys are stored in encrypted form to prevent access.
FPT_APW_EXT.1	All admin passwords are stored as a hash values instead of in plaintext form to ensure admin passwords are not readable even to administrators.
FPT_STM.1	All forms of the TOE use their software clocks to provide timestamps written to audit records, and to track inactivity of administrative sessions. The TOEs that include hardware clocks (4300 series and 4500 series sensors) retain time and date across power-cycles. The TOEs that do not include hardware-clocks (the IPS SSP hardware module and software module) obtain the time and date for their software clocks from the hardware clock of the underlying ASA host. All forms of the TOE can optionally be set to receive clock updates from an NTP server.
FPT_TUD_EXT.1	The TOE software version and hardware components can be queried by an administrator. When updates are made available by Cisco, an administrator can obtain and install those updates. An administrator can download software updates to the TOE then generate cryptographic hash values and compare those hash values to published (known-good) hash values to verify software/firmware update files have not been modified from the originals distributed by Cisco before the files are used to update the applicable TOE components.
FPT_TST_EXT.1	As a FIPS 140-2 validated product, the TOE runs a suite of self-tests during initial start-up to verify its correct operation. Refer to the FIPS Security Policy for available options and management of the cryptographic self-test. For testing of the TSF, the TOE automatically runs checks and power-on self-tests (POST) during startup and resets to ensure the TOE is operating correctly. The self tests include verification of cryptographic module functions. Success and failure notifications are output to the console during startup, and failure of cryptographic

TOE SFRs	How the SFR is Satisfied
	tests will cause the device to shut down and restart the POST. The cryptographic self tests include Known Answer Testing (KAT) to verify that, given known inputs, the correct results are produced by the cryptographic modules.
FTA_SSL_EXT.1 FTA_SSL.3	An administrator can configure maximum inactivity times individually for both local and remote administrative sessions. When a session is inactive (i.e., no session input from the administrator) for the configured period of time the TOE will terminate the session requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session.
FTA_SSL.4	Administrators are able to exit out (logout) of both local and remote administrative sessions, terminating the authenticated session.
FTA_TAB.1	The TOE displays a banner at time of logon via the CLI and GUI. Administrators can customize the banner text.
FTP_ITC.1	When configured by an Administrator to dynamically modify access control lists on compatible network traffic blocking and rate-limiting devices such as routers, switches, and firewalls, the TOE supports initiation of SSH connections to those network devices. The TOE supports remote retrieval of audit records (event logs) over TLS/HTTPS connections initiated to the TOE from authorized and authenticated remote systems. The TOE can initiate connections over SCP (SSH), or TLS/HTTPS to copy iplogs (logs of IPS events, not “event logs”) to remote systems. The TOE can initiate SCP (SSH) or TLS/HTTPS connections to download IPS signature file updates or other files.
FTP_TRP.1	All remote administrative communications take place over a secure encrypted SSH or TLS/HTTPS session initiated by remote administrators. The SSH sessions and TLS sessions are secured using AES encryption and SHA hashing.

6.3 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, a CLI 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 access control. In order to 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.

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.

7 SUPPLEMENTAL CRYPTOGRAPHIC INFORMATION

7.1 Key Zeroization

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

Table 24: TOE Key Zeroization

Critical Security Parameters (CSPs)	Zeroization Cause and Effect
Diffie-Hellman Shared Secret	Automatically 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	Zeroized upon completion of DH exchange, by calling a specific API within the two crypto modules, when module is shutdown, or reinitialized. Overwritten with: 0x00
SSH Private Key	Generation of a new key Overwritten with: 0x00
SSH Session Key	Automatically when the SSH session is terminated. Overwritten with: 0x00

7.2 NIST Special Publication 800-56A

The TOE is compliant with NIST SP 800-56A as described in Table 25 below.

Table 25 800-56A Compliance

Section	Exceptions to 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 Number	None.	None.	Yes	N/A

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

Section	Exceptions to Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
Generation				
5.4 Nonces	None.	"a random nonce **should** be used"	Yes	N/A
5.5 Domain Parameters	None.	None.	Yes	N/A
5.5.1 Domain Parameter Generation	N/A, no shall statements	"If the appropriate security strength does not have an FFC parameter set, then Elliptic Curve Cryptography **should** be used"	Yes	N/A
5.5.1.1 FFC Domain Parameter Generation	None.	None.	Yes	N/A
5.5.1.2 ECC Domain Parameter Generation	N/A, no ECC in use.	None.	N/A	TOE does not use ECC.
5.5.2 Assurances of Domain Parameter Validity	None.	None.	Yes	N/A
5.5.3 Domain Parameter Management	None.	None.	Yes	N/A
5.6 Private and Public Keys	N/A, no shall statements	None.	Yes	N/A
5.6.1 Private/Public Key Pair Generation	N/A, no shall statements	None.	Yes	N/A
5.6.1.1 FFC Key Pair Generation	None.	None.	No	N/A
5.6.1.2 ECC Key Pair Generation	N/A, no ECC in use.	None.	N/A	TOE does not use ECC.
5.6.2 Assurances of the Arithmetic Validity of a Public Key	None.	None.	Yes	N/A
5.6.2.1 Owner Assurances of Static Public Key Validity	None. Static key is not supported.	None.	Yes	N/A
5.6.2.2 Recipient Assurances of Static Public Key Validity	None. Static key is not supported.	None.	Yes	N/A
5.6.2.3 Recipient Assurances of Ephemeral Public Key Validity	None.	None.	Yes	N/A
5.6.2.4 FFC Full Public Key Validation Routine	None.	None.	Yes	N/A
5.6.2.5 ECC Full Public Key Validation Routine	N/A, no ECC in use.	None.	N/A	TOE does not use ECC.
5.6.2.6 ECC Partial Public Key Validation Routine	N/A, no ECC in use.	None.	N/A	TOE does not use ECC.
5.6.3 Assurances of the Possession of a Static	None. Static key is not supported.	None.	Yes	N/A

Section	Exceptions to Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
Private Key				
5.6.3.1 Owner Assurances of Possession of a Static Private Key	None. Static key is not supported.	None.	Yes	N/A
5.6.3.2 Recipient Assurance of Owner's Possession of a Static Private Key	None. Static key is not supported.	None.	Yes	N/A
5.6.3.2.1 Recipient Obtains Assurance through a Trusted Third Party	N/A, no shall statements	None.	Yes	N/A
5.6.3.2.2 Recipient Obtains Assurance Directly from the Claimed Owner	None. Static key is not supported.	None.	Yes	N/A
5.6.4 Key Pair Management	N/A, no shall statements	None.	Yes	N/A
5.6.4.1 Common Requirements on Static and Ephemeral Key Pairs	None.	None.	Yes	N/A
5.6.4.2 Specific Requirements on Static Key Pairs	None. Static key is not supported.	None.	Yes	N/A
5.6.4.3 Specific Requirements on Ephemeral Key Pairs	None.	"An ephemeral key pair **should** be generated as close to its time of use as possible"	Yes	N/A
5.7 DLC Primitives	None.	None.	Yes	N/A
5.7.1 Diffie-Hellman Primitives	N/A, no shall statements	None.	Yes	N/A
5.7.1.1 Finite Field Cryptography Diffie-Hellman (FFC DH) Primitive	N/A, no shall statements	None.	Yes	N/A
5.7.1.2 Elliptic Curve Cryptography Cofactor Diffie-Hellman (ECC CDH) Primitive	N/A, no shall statements	None.	N/A	TOE does not use ECC.
5.7.2 MQV Primitives	N/A, no shall statements	None.	Yes	N/A
5.7.2.1 Finite Field Cryptography MQV (FFC MQV) Primitive	N/A, no shall statements	None.	Yes	N/A
5.7.2.1.1 MQV2 Form of the FFC MQV Primitive	N/A, no shall statements	None.	Yes	N/A
5.7.2.1.2 MQV1 Form	N/A, no shall	None.	Yes	N/A

Section	Exceptions to Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
of the FFC MQV Primitive	statements			
5.7.2.2 ECC MQV Associate Value Function	N/A, no shall statements	None.	N/A	TOE does not use ECC.
5.7.2.3 Elliptic Curve Cryptography MQV (ECC MQV) Primitive	N/A, no shall statements	None.	N/A	TOE does not use ECC.
5.7.2.3.1 Full MQV Form of the ECC MQV Primitive	N/A, no shall statements	None.	N/A	TOE does not use ECC.
5.7.2.3.2 One-Pass Form of the ECC MQV Primitive	N/A, no shall statements	None.	N/A	TOE does not use ECC.
5.8 Key Derivation Functions for Key Agreement Schemes	In TLS the MAC key is used for traffic protection as well as key confirmation.	None.	No	Only applicable if Key Confirmation (KC) or implementation validation testing are to be performed as specified in Section 8.
5.8.1 Concatenation Key Derivation Function (Approved Alternative 1)	See above.	None.	Yes	Only applicable if If Key Confirmation (KC) or implementation validation testing are to be performed as specified in Section 8.
5.8.2 ASN.1 Key Derivation Function (Approved Alternative 2)	See above.	None.	Yes	Only applicable if If Key Confirmation (KC) or implementation validation testing are to be performed as specified in Section 8.
6. Key Agreement	None.	None.	Yes	N/A
6.1 Schemes Using Two Ephemeral Key Pairs, C(2)	N/A, no shall statements	None.	Yes	N/A
6.1.1 Each Party Has a Static Key Pair and Generates an Ephemeral Key Pair, C(2, 2)	None.	None.	N/A	N/A, TOE uses C(2,0)
6.1.1.1 dhHybrid1, C(2, 2, FFC DH)	None.	None.	N/A	TOE uses C(2,0)
6.1.1.2 Full Unified Model, C(2, 2, ECC CDH)	N/A, no ECC in use.	None.	N/A	TOE does not use ECC. TOE would use C(2,0)
6.1.1.3 MQV2, C(2, 2, FFC MQV)	None.	None.	N/A	N/A, TOE uses C(2,0)
6.1.1.4 Full MQV, C(2, 2, ECC MQV)	N/A, no ECC in use.	None.	N/A	TOE does not use ECC. TOE would use C(2,0)
6.1.1.5 Rationale for Choosing a C(2, 2) Scheme	N/A, no shall statements	None.	N/A	N/A, TOE uses C(2,0)

Section	Exceptions to Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
6.1.2 Each Party Generates an Ephemeral Key Pair; No Static Keys are Used, C(2, 0)	None.	None.	Yes	N/A
6.1.2.1 dhEphem, C(2, 0, FFC DH)	None.	None.	Yes	N/A
6.1.2.2 Ephemeral Unified Model, C(2, 0, ECC CDH)	N/A, no ECC in use.	None.	N/A	TOE does not use ECC.
6.1.2.3 Rationale for Choosing a C(2, 0) Scheme	N/A, no shall statements	None.	Yes	N/A
6.2 Schemes Using One Ephemeral Key Pair, C(1)	N/A, no shall statements	None.	N/A	N/A, TOE uses C(2,0)
6.2.1 Initiator Has a Static Key Pair and Generates an Ephemeral Key Pair; Responder Has a Static Key Pair, C(1, 2)	None.	None.	N/A	N/A, TOE uses C(2,0)
6.2.1.1 dhHybridOneFlow, C(1, 2, FFC DH)	None.	None.	N/A	N/A, TOE uses C(2,0)
6.2.1.2 One-Pass Unified Model, C(1, 2, ECC CDH)	N/A, no ECC in use.	None.	N/A	TOE does not use ECC. TOE would use C(2,0)
6.2.1.3 MQV1, C(1, 2, FFC MQV)	None.	None.	N/A	N/A, TOE uses C(2,0)
6.2.1.4 One-Pass MQV, C(1, 2, ECC MQV)	N/A, no ECC in use.	None.	N/A	TOE does not use ECC. TOE would use C(2,0)
6.2.1.5 Rationale for Choosing a C(1, 2) Scheme	N/A, no shall statements	None.	N/A	N/A, TOE uses C(2,0)
6.2.2 Initiator Generates Only an Ephemeral Key Pair; Responder Has Only a Static Key Pair, C(1, 1)	None.	None.	N/A	N/A, TOE uses C(2,0)
6.2.2.1 dhOneFlow, C(1, 1, FFC DH)	None.	None.	N/A	N/A, TOE uses C(2,0)
6.2.2.2 One-Pass Diffie-Hellman, C(1, 1, ECC CDH)	N/A, no ECC in use.	None.	N/A	TOE does not use ECC. TOE would use C(2,0)
6.2.2.3 Rationale in Choosing a C(1, 1) Scheme	N/A, no shall statements	None.	N/A	N/A, TOE uses C(2,0)
6.3 Scheme Using No Ephemeral Key Pairs,	None.	None.	N/A	N/A, TOE uses C(2,0)

Section	Exceptions to Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
C(0, 2)				
6.3.1 dhStatic, C(0, 2, FFC DH)	N/A, no shall statements	None.	N/A	N/A, TOE uses C(2,0)
6.3.2 Static Unified Model, C(0, 2, ECC CDH)	N/A, no ECC in use.	None.	N/A	TOE does not use ECC. TOE would use C(2,0)
6.3.3 Rationale in Choosing a C(0, 2) Scheme	N/A, no shall statements	None.	N/A	N/A, TOE uses C(2,0)
7. DLC-Based Key Transport	None.	None.	Yes	TOE uses C(2,0)
8. Key Confirmation	None.	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.1 Assurance of Possession Considerations when using Key Confirmation	None.	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.2 Unilateral Key Confirmation for Key Agreement Schemes	None.	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.3 Bilateral Key Confirmation for Key Agreement Schemes	N/A, no shall statements	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4 Incorporating Key Confirmation into a Key Agreement Scheme	None.	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4.1 C(2, 2) Scheme with Unilateral Key Confirmation Provided by U to V	N/A, no shall statements	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4.2 C(2, 2) Scheme with Unilateral Key Confirmation Provided by V to U	N/A, no shall statements	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4.3 C(2, 2) Scheme with Bilateral Key Confirmation	N/A, no shall statements	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4.4 C(1, 2) Scheme	None.	None.	Yes	Key confirmation for the

Section	Exceptions to Shall/Shall Not Statement(s)	Should (Not) Statements[1]	TOE Compliant?	Rationale
with Unilateral Key Confirmation Provided by U to V				C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4.5 C(1, 2) Scheme with Unilateral Key Confirmation Provided by V to U	N/A, no shall statements	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4.6 C(1, 2) Scheme with Bilateral Key Confirmation	None.	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4.7 C(1, 1) Scheme with Unilateral Key Confirmation Provided by V to U	N/A, no shall statements	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4.8 C(0, 2) Scheme with Unilateral Key Confirmation Provided by U to V	None.	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4.9 C(0, 2) Scheme with Unilateral Key Confirmation Provided by V to U	N/A, no shall statements	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair
8.4.10 C(0, 2) Scheme with Bilateral Key Confirmation	None.	None.	Yes	Key confirmation for the C(2, 0) key agreement schemes is not specified, since neither party has a static key pair

7.3 NIST Special Publication 800-56B

The TOE is compliant with NIST SP 800-56B as described in Table 26 below.

Table 26 800-56B Compliance

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[2]	TOE Compliant?	Rationale
5 Cryptographic	None.	None.	Yes	N/A

[2] 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[2]	TOE Compliant?	Rationale
Elements				
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 Derivation Function (Approved Alternative 2)	None.	None.	Yes	N/A
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

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[2]	TOE Compliant?	Rationale
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 Key Validity	None.	None.	Yes	N/A
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

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[2]	TOE Compliant?	Rationale
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
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	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	Yes	N/A

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[2]	TOE Compliant?	Rationale
Scheme (RSA-KEM-KWS)		from one another by an opponent, whether by error message or timing." "A single error message **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
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	Yes	N/A

Section	Shall/Shall Not Statement(s)	Should (Not) Statements[2]	TOE Compliant?	Rationale
		secret Z."		
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 KTS-KEM-KWS Schemes	N/A, no shall statements	None.	Yes	N/A
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

8 ANNEX A: REFERENCES

The following documentation was used to prepare this ST.

Table 27: 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-2012-09-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-004
[NDPP]	U.S. Government Protection Profile for Security Requirements for Network Devices, version 1.1, June 8, 2012
[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