Cisco Catalyst Switches (3560C, 3560X and 3750X) Running IOS 15.0(2)SE4 Security Target

Revision 1.0

16 January 2014

Table of Contents

List of Tables

List of Figures

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 Cisco Catalyst Switches (3560C, 3560X and 3750X) running IOS 15.0(2)SE4. 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.

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 3, Chapter 4.

1.1 ST and TOE Reference

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

Table 1: ST and TOE Identification

ST Title	Cisco Catalyst Switches (3560C, 3560X and 3750X) Running IOS 15.0(2)SE4 Security Target
ST Version	1.0
Publication Date	16 January 2014
ST Author	Cisco Systems, Inc.
Developer of the TOE	Cisco Systems, Inc.
TOE Reference	Cisco Catalyst Switches (3560C, 3560X and 3750X)
TOE Hardware Models	Cisco Catalyst Switches 3560C, 3560X and 3750X
TOE Software Version	IOS 15.0(2)SE4
ST Evaluation Status	In Evaluation
Keywords	Audit, Authentication, Encryption, Protection, Switch, Traffic

1.2 Acronyms and Abbreviations

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

Table 2: Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
BGP	Border Gateway Protocol. An exterior gateway protocol. It performs routing between multiple autonomous systems and exchanges routing and reachability information with other BGP systems.
CC	Common Criteria for Information Technology Security Evaluation

Acronyms / Abbreviations	Definition
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
DH	Diffie-Hellman
EAL	Evaluation Assurance Level
EEPROM	Electrically erasable programmable read-only memory, specifically the memory in the switch where the Cisco IOS is stored.
EIGRP	Enhanced Interior Gateway Routing Protocol
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
HTTPS	Hyper-Text Transport Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IOS	The proprietary operating system developed by Cisco Systems.
IP	Internet Protocol
IPsec	IP Security
IT	Information Technology
MAC	Media Access Control
NTP	Network Time Protocol
NVRAM	Non-volatile random access memory, specifically the memory in the switch where the configuration parameters are stored.
OS	Operating System
OSPF	Open Shortest Path First. An interior gateway protocol (routes within a single autonomous system). A link-state routing protocol which calculates the shortest path to each node.
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
PIM-SM	Protocol Independent Multicast – Sparse Mode
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PVLAN	Private VLAN
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol. An interior gateway protocol (routes within a single autonomous system). A distance-vector protocol that uses hop count as its metric.
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SM	Service Module
SSH	Secure Shell
SSHv2	Secure Shell (version 2)
ST	Security Target
TACACS	Terminal Access Controller Access Control System
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TOE	Target of Evaluation

Acronyms / Abbreviations	Definition
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User Datagram Protocol
VACL	Virtual Access Control List
VLAN	Virtual Local Area Network
VSS	Virtual Switching System

1.3 TOE Overview

The TOE is the Cisco Catalyst Switches (3560C, 3560X and 3750X) running IOS 15.0(2)SE4 (herein after referred to as Catalyst Switches). The TOE is a purpose-built, switching and routing platform with OSI Layer2 and Layer3 traffic filtering capabilities.

Cisco IOS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS performs many networking functions, this Security Target only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 TOE logical scope below.

1.3.1 TOE Product Type

The Cisco Catalyst Switches are a switching and routing platform used to construct IP networks by interconnecting multiple smaller networks or network segments. As a Layer2 switch, it performs analysis of incoming frames, makes forwarding decisions based on information contained in the frames, and forwards the frames toward the destination. As a Layer3 switch, it supports routing of traffic based on tables identifying available routes, conditions, distance, and costs to determine the best route for a given packet. Routing protocols used by the TOE include BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 and RIPv2. The routing protocols, BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 supports routing updates with IPv4 or IPv6, while RIPv2 routing protocol support routing updates for IPv4 only. Although IOS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 Logical Scope of the TOE below.

1.3.2 Supported non-TOE Hardware/ Software/ Firmware

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

Table 3: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Authentication Server	Yes	This includes any authentication server (RADIUS RFC 2865, 2866, 2869 and RFC 3162 (IPv6) and TACACS+ RFC 1492)) that can be leveraged for remote user authentication. The AAA server needs to be able of acting as an IPsec peer or as an IPsec endpoint.
Management	Yes	This includes any IT Environment Management

Component	Required	Usage/Purpose Description for TOE performance
Workstation		workstation that is used by the TOE administrator to support TOE administration through protected channels (e.g. IPsec).
Audit (syslog) server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. The TOE would ensure that messages are encrypted within an IPsec tunnel as they leave the TOE. The syslog server needs to be able of acting as an IPsec peer or as an IPsec endpoint.
NTP Server	No	The TOE supports communications with an NTP server to receive clock updates. Any server that supports NTPv1 (RFC 1059), NTPv2 (RFC 1119), or NTP v3 (RFC 1305) may be used.

1.4 TOE DESCRIPTION

The Catalyst Switches that comprise the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware.

The Cisco Catalyst 3560C Series are small-factor; fixed configuration switches offering Fast Ethernet and Gigabit Ethernet connectivity for extending Cisco Catalyst wired switching infrastructure and wireless LAN networks. The main features are:

- Fixed-configuration switches.
- Layer 2 switching with intelligent Layer 2 – 4 services for voice, video and wireless LAN services.
- Fast Ethernet and Gigabit Ethernet connectivity.
- Power over Ethernet (PoE) pass-through enables the compact switch to draw power from the wiring closet and pass it to end devices (selected models)
- Fanless operation.

The Cisco Catalyst 3560X and 3750X Series Switches are enterprise-class line of stackable and stand-alone switches respectively. They provide high availability, scalability, security, energy efficiency, IEEE 802.3at Power over Ethernet Plus (PoE+) configurations, optional network modules, redundant power supplies, and Media Access Control Security (MACsec) features. The Cisco Catalyst 3750-X and 3560-X enhance productivity by enabling applications such as IP telephony, wireless, and video for borderless network experience.

The Cisco Catalyst 3560X and 3750X primary features are:

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operations
- Flash memory (EEPROM), used to store the Cisco IOS image (binary program)
- USB port (note, none of the USB devices are included in the TOE)
    - Type A for Storage, all Cisco supported USB flash drives

    - Type mini-B as console port in the front
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs
- Non-volatile random-access memory (NVRAM) is used to store switch configuration parameters used to initialize the system at start-up
- Physical network interfaces (minimally two) (e.g. RJ45 serial and standard 10/100 Ethernet ports). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces
- 24 and 48 10/100/1000 PoE+, non-PoE models, and 12 and 24 GE SFP port models
- Four optional uplink network modules with GE or 10GE ports
- PoE+ with 30W power on all ports in 1 rack unit (RU) form factor
- Dual redundant, modular power supplies and fans

In addition to the above features, the Cisco Catalyst 3750-X switches also offer:

- Cisco StackPower™ technology: An innovative feature for sharing power among stackmembers
- Cisco StackWise Plus technology for ease of use and resiliency with 64 Gbps of throughput

Cisco IOS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 Logical Scope of the TOE below.

1.5 TOE Environment and Configuration

The TOE consists of one or more physical devices; the Catalyst Switch with Cisco IOS software. All of the Catalyst Switches run the same version of the IOS 15.0(2)SE4 (FIPS Validated) software which enforces the security functions being claimed regardless of the model.

The Catalyst Switch has two or more network interfaces and is connected to at least one internal and one external network.

The Cisco IOS software configuration determines how packets are handled to and from the switches' network interfaces. The switch configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination. BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 and RIPv2, Routing protocols are used on all of the Catalyst Switch models. Note, the information flow functionality is not included in the scope of the evaluation. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in this Security Target (ST). For example,

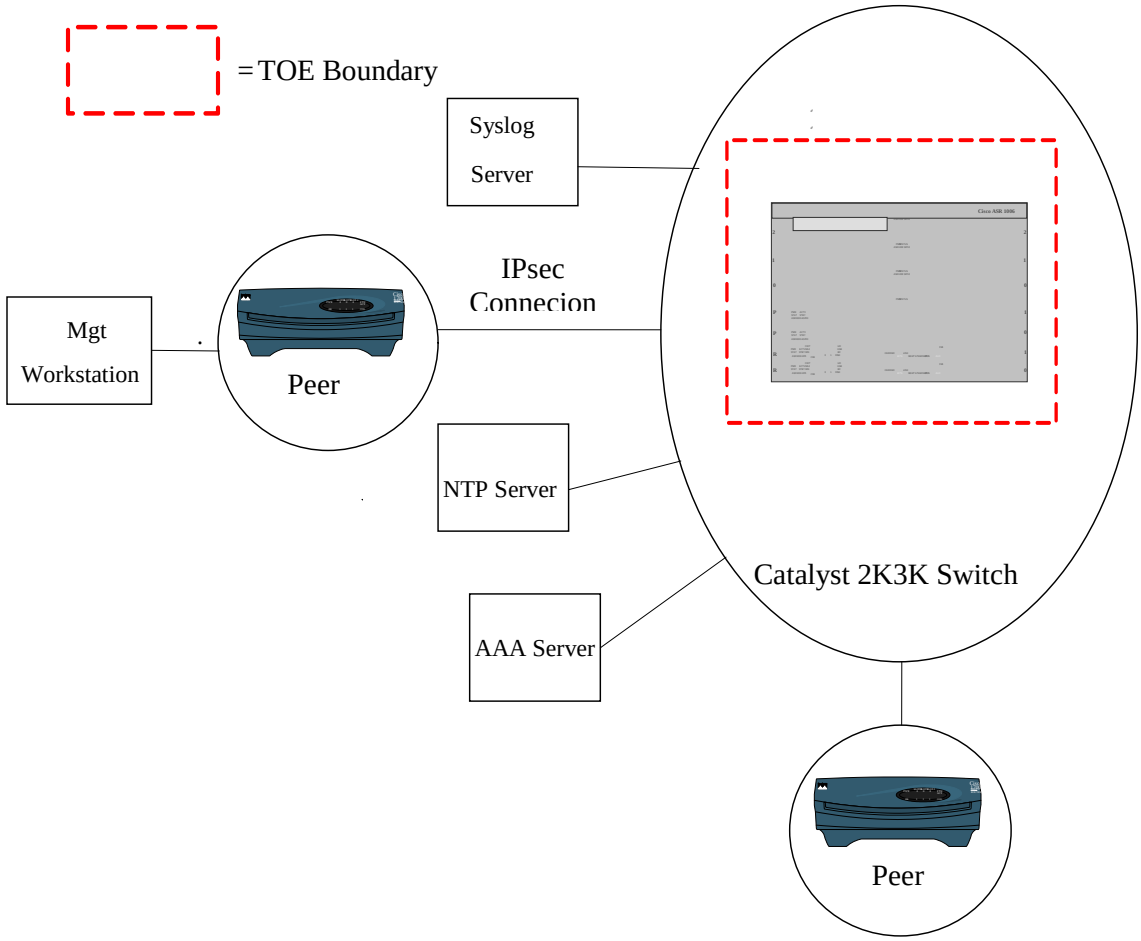
- Security audit – ensures that audit records are generated for the relevant events and are securely transmitted to a remote syslog server using IPsec
- Cryptographic support – ensures cryptography support for secure communications
- User Data Protection - ensures that packets transmitted from the TOE do not contain residual information from previous packets
- Identification and authentication – ensures a warning banner is displayed at login, that all users are successfully identified and authenticated prior to gaining access to the TOE, the users can only perform functions in which they have privileges, and terminates users after a configured period of inactivity

- Secure Management – ensures secure administrative services for management of general TOE configuration and the security functionality provided by the TOE
- Protection of the TSF - provides secure transmission when TSF data is transmitted between the TOE and other IT entities, is also able to detect replay of information received via secure channels (e.g. IPsec), ensures updates have not been modified and are from a trusted source and maintains the date and time. that is used as the timestamp applied to audit records
- Resource Utilization - capability of controlling and managing resources so that a denial of service will not occur
- TOE access - ensures inactive sessions are terminated after an authorized administrator configurable time-period
- Trusted Path/Channel - a trusted path between the TOE and the CLI using SSHv2, over IPsec tunnel, with the syslog server and if configured with the NTP server and external authentication server using IPsec

The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the Catalyst Switch is to be remotely administered, then the management station must be connected to an internal network, a secure IPsec tunnel must be used to connect to the switch. A syslog server can also be used to store audit records. A remote authentication server can also be used for centralized authentication. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

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

Figure 1: TOE Deployment Example



1.6 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the following switch models; Cisco Catalyst 3560C, 3560X and 3750X all running IOS 15.0(2)SE4. Each Switch is running the same version of the IOS 15.0(2)SE4 (FIPS Validated) software which enforces the security functions being claimed regardless of the model. The network, on which they reside, is part of the environment.

The physical network interfaces to the switch are Ethernet interfaces receiving and transmitting Internet Protocol datagrams as specified in RFC 0894 [Ethernet], RFC 0791 [IPv4], and RFC 2460 [IPv6]. Over this physical interface network traffic packets are transferred into and out of the TOE. The physical network interface (ports) can be located on the supervisor card and/or the line cards.

The network interface is the physical Ethernet interface to the TOE from the internal and external networks. Within the scope of the evaluation, this interface is used for the following purposes:

- For network traffic entering and leaving the TOE. This could be 'through traffic' for example a telnet packet from a user destined from an internal network to an external network, or 'to the box traffic' for example an external ping to the TOE's IP address.
- To allow a remote Administrator to access the TOE's CLI over the network using SSHv2 over IPsec.
- To allow the audit log records to be transmitted to the syslog server via IPsec connection tunnel.
- To allow, if configured, time synchronization with the NTP server via secure transmission (IPsec).
- To allow, if configured, the TOE access to the AAA server to authenticate TOE administrators via secure transmission (IPsec).

1.6.1 Cat 3560C Switches

The Cisco Catalyst 3560C Series are fixed compact switches that offer enhanced intelligent services that include comprehensive Layer 2 features and also includes the support for routed access, MACsec (provides Layer 2, line rate Ethernet data confidentiality and integrity on host facing ports, protecting against man-in-the-middle attacks like snooping, tampering, and replay), and Open Shortest Path First (OSPF).

Figure 2: Cisco Catalyst 3560-C Series Switches

Table 4: Configurations of Cisco Catalyst 3560-C Series Switches

Catalyst 3560-C Switch Model	Description	PoE Output Ports and available PoE Power	Uplinks	MACsec
Cisco Catalyst 3560C-8PC-S	8 x 10/100 Fast Ethernet	8 PoE+, 124W	2 x 1G copper or 1G SFP	Yes
Cisco Catalyst 3560C-12PC-S	12 x 10/100 Fast Ethernet	12 PoE+, 124W	2 x 1G copper or 1G SFP	Yes
Cisco Catalyst 3560CG-8TC-S	8 x 10/100/1000 Gigabit Ethernet	N/A	2 x 1G copper or 1G SFP	Yes

Catalyst 3560-C Switch Model	Description	PoE Output Ports and available PoE Power	Uplinks	MACsec
Cisco Catalyst 3560CG-8PC-S	8 x 10/100/1000 Gigabit Ethernet	8 PoE+, 124W	2 x 1G copper or 1G SFP	Yes
Cisco Catalyst 3560CPD-8PT-S	8 x 10/100/1000 Gigabit Ethernet	8 PoE, Up to 15.4W	2 x 1G (PoE+ input)	Yes

1.6.2 Cat 3560X and 3750X Switches

The Catalyst 3560X and 3750X Switches offers enhanced intelligent services that include comprehensive Layer 2 features, with up-to 1K VLANs, with the addition of support for baseline enterprise services, routed access, StackPower (available only on the Catalyst 3750-X), advanced Layer 3 features such as Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Protocol Independent Multicast (PIM), Routing Information Protocol (RIPv2), and IPv6 routing such as OSPFv3 and EIGRPv6. Note, the information flow functionality is not included in the scope of the evaluation. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in this Security Target (ST) in Section 5.

Figure 3: The Cisco Catalyst 3560-X Series Configurations

Table 5: Configurations of Cisco Catalyst 3560-X Series Switches

	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
	WS-C3560-X-24T-L/Standalone	24	350W	-
	WS-C3560-X-48T-	48		

	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
	L/Standalone			
	WS-C3560-X-24P-L/Standalone	24 PoE+	715W	435W
	WS-C3560-X-48P-L/Standalone	48 PoE+		
	WS-C3560-X-48PF-L/Standalone	48 PoE+	1100W	800W
	WS-C3560-X-24T-S/Standalone	24	350W	-
	WS-C3560-X-48T-S/Standalone	48		
	WS-C3560-X-24P-S/Standalone	24 PoE+	715W	435W
	WS-C3560-X-48P-S/Standalone	48 PoE+		
	WS-C3560-X-48PF-S/Standalone	48 PoE+	1100W	800W

Figure 4: The Cisco Catalyst 3750-X Series Configurations – Front and back view

Table 6: The Cisco Catalyst 3750-X Series Configurations

	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
	WS-C3750X-24T-L/Stackable (stackpower	24	350W	-

	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
	available with upgrade to IPBase)			
	WS-C3750X-48T-L/Stackable	48		
	WS-C3750X-24P-L/Stackable	24 PoE+	715W	435W
	WS-C3750X-48P-L/Stackable	48 PoE+		
	WS-C3750X-48PF-L/Stackable	48 PoE+	1100W	800W
	WS-C3750X-24T-S/Stackable (stack power)	24	350W	-
	WS-C3750X-48T-S/Stackable	48		
	WS-C3750X-24P-S/Stackable	24 PoE+	715W	435W
	WS-C3750X-48P-S/Stackable	48 PoE+		
	WS-C3750-X-48PF-S/Stackable	48 PoE+	1100W	800W
	WS-C3750-X-12S-E/Stackable	12 GE SFP	350W	-
	WS-C3750-X-24S-E/Stackable	24 GE SFP	350W	

Figure 5: StackPower Connector

StackPower can be deployed in either power sharing mode or redundancy mode. In power sharing mode, the power of all the power supplies in the stack is aggregated and distributed among the switches in the stack. In redundant mode, when the total power budget of the stack is calculated, the wattage of the largest power supply is not included. That power is held in reserve and used to maintain power to switches and attached devices when one power supply fails, enabling the

network to operate without interruption. Following the failure of one power supply, the StackPower mode becomes power sharing.

StackPower allows customers to simply add one extra power supply in any switch of the stack and provide either power redundancy for any of the stack members or simply add more power to the shared pool. StackPower eliminates the need for an external redundant power system or installation of dual power supplies in all the stack members. Note, power sharing is a feature of the product with no specific requirements included in the scope of the evaluation. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in this Security Target (ST) in Section 5.

1.7 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. User data protection
4. Identification and authentication
5. Secure Management
6. Protection of the TSF
7. Resource Utilization
8. TOE access
9. Trusted path/channels

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

1.7.1 Security audit

The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include; modifications to the group of users that are part of the authorized administrator roles, all use of the user identification mechanism, any use of the authentication mechanism, any change in the configuration of the TOE.

The TOE is configured to store the audit logs on an external syslog server. Communication with the syslog server is protected using IPsec and the TOE can determine when communication with the syslog server fails. If that should occur, the TOE can be configured to block new permit actions.

The logs can be viewed on the TOE using the appropriate IOS commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to delete audit data stored locally on the TOE

1.7.2 Cryptographic support

The TOE provides cryptography support for secure communications and protection of information when configured in FIPS mode. The crypto module is FIPS 140-2 SL2 validated (Certificate 1940/IOS Common Cryptographic Module (IC2M) (Firmware Versions: **Rel 1(1.0.0)**, Rel 1(1.0.1) and Rel 1(1.0.2)). The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; digital signature using RSA; cryptographic hashing using SHA1; keyed-hash message authentication using HMAC-SHA1, and IPsec for authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE also implements IPsec secure protocol for secure remote administration. In the evaluated configuration, the TOE must be operated in FIPS mode of operation per the FIPS Security Policy (Certificate 1940/IOS Common Cryptographic Module (IC2M) (Firmware Versions: **Rel 1(1.0.0)**, Rel 1(1.0.1) and Rel 1(1.0.2)).

1.7.3 User Data Protection

The TOE also ensures that packets transmitted from the TOE do not contain residual information from previous packets. Packets that are not the required length use zeros for padding so that residual data from previous traffic is never transmitted from the TOE.

1.7.4 Identification and authentication

The TOE performs authentication, using Cisco IOS platform authentication mechanisms, to authenticate access to user EXEC and privileged EXEC command modes. All users wanting to use TOE services are identified and authenticated prior to being allowed access to any of the services. Once a user attempts to access the management functionality of the TOE (via EXEC mode), the TOE prompts the user for a user name and password. Only after the administrative user presents the correct identification and authentication credentials will access to the TOE functionality be granted.

The TOE optionally also supports use of a remote AAA server (RADIUS and TACACS+) as the enforcement point for identifying and authenticating users attempting to connect to the TOE's CLI. Note the remote authentication server is not included within the scope of the TOE evaluated configuration, it is considered to be provided by the operational environment.

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

1.7.5 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 session via IPsec, a terminal server directly connected to the Catalysis Switch (RJ45), or a local console connection (serial port). The TOE provides the ability to perform the following actions:

- allows authorized administrators to add new administrators,
- start-up and shutdown the device,
- create, modify, or delete configuration items,
- modify and set session inactivity thresholds,
- modify and set the time and date,

- and create, delete, empty, and review the audit trail

All of these management functions are restricted to the authorized administrator of the TOE.

The term “authorized administrator” is used in this ST to refer to any administrative user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions.

1.7.6 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 IOS is not a general purpose operating system and access to Cisco IOS memory space is restricted to only Cisco IOS functions.

The TOE provides secure transmission when TSF data is transmitted between the TOE and other IT entities, such as remote administration and secure transmission of the audit logs via IPsec.

The TOE is also able to detect replay of information and/or operations. The detection applied to network packets that are terminated at the TOE, such as trusted communications between the administrators to TOE, IT entity (e.g., authentication server) to TOE. If replay is detected, the packets are discarded.

In addition, the TOE internally maintains the date and time. This date and time is used as the time stamp that is applied to TOE generated audit records. Alternatively, an NTP server can be used to synchronize the date-timestamp. Finally, the TOE performs testing to verify correct operation of the switch itself and that of the cryptographic module.

1.7.7 Resource utilization

The TOE provides the capability of controlling and managing resources so that a denial of service will not occur. The resource allocations are configured to limit the number of concurrent administrator sessions.

1.7.8 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 also provides the administrator with the ability to display a notification of use banner on the CLI management interface prior to allowing any administrative access to the TOE.

1.7.9 Trusted Path/Channels

The TOE establishes a trusted path between the appliance and the CLI, syslog server, NTP server and if configured, an external authentication server using IPsec.

1.8 Excluded Functionality

The Cisco IOS contains a collection of features that build on the core components of the system. Those features that are not within the scope of the evaluated configuration include:

- HTTP or HTTPS Server - The IOS web server (using HTTPS or HTTP) cannot satisfy all the NDPP requirements for administrative interfaces and must remain disabled in the evaluated configuration. The CLI interface is used to manage the TOE. Not including this feature does not interfere with the management of TOE as defined in the Security Target or the operation of the TOE Refer to the Guidance documentation in Section 1.9 for configuration syntax and information.
- IEEE 802.11 Wireless Standards requires additional hardware beyond what is included in the evaluated configuration.
- SNMP does not enforce the required privilege levels. This feature is disabled by default and cannot be configured for use in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target. The exclusion of this feature has no effect on the operation of the TOE.
- Telnet sends authentication data in the clear. This feature is enabled by default and must be disabled in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target. The exclusion of this feature has no effect on the operation of the TOE.
- VPN Remote Access requires additional licenses beyond what is included in the evaluated configuration. Administrative remote access is secured using IPsec.
- TrustSec is only relevant to this ST to a limited degree, for RADIUS KeyWrap, which is being represented with other cryptographic methods, such as AES and IPsec. This feature is disabled by default and should remain disabled in the evaluated configuration. Not including this feature does not interfere with the enforcement of the security policies as defined in the Security Target.
- Smart Install is a feature to configure IOS Software and switch configuration without user intervention. The Smart Install uses dynamic IP address allocation to facilitate installation providing transparent network plug and play. This feature is not to be used as it could result in settings/configurations that would as it may interfere with the enforcement of the security policies as defined in the Security Target.
- The TOE supports routing protocols including BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 and RIPv2 to maintain routing tables, or routing tables can configured and maintained manually (‘static routes’). Since routing tables are used to determine which egress ACL is applied to the outbound traffic, the authority to modify the routing tables is restricted to authenticated administrators, and authenticated neighbor routers.
- The TOE also supports authentication of other routers using router authentication supported by BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 and RIPv2. Each of these protocols supports authentication by transmission of MD5-hashed password strings, which each neighbor router uses to authenticate others. It is noted that per the FIPS Security Policy, that MD5 is not a validated algorithm during FIPS mode of operation. For additional security, it is recommended router protocol traffic also be isolated to separate VLANs.

Apart from these exceptions, all types of network traffic through and to the TOE are within the scope of the evaluation.

1.9 TOE Documentation

This section identifies the guidance documentation included in the TOE. The documentation for the Cisco Catalyst Switches (3560C, 3560-X and 3750-X) comprises:

- Installation and Configuration for Common Criteria NDPP V1.0 Evaluated Cisco IOS Catalyst Switches (3560C, 3560-X and 3750-X)
- Administrative Guidance for Cisco Catalyst Switches 3560C, 3560-X and 3750-X)
- Cisco IOS Security Command Reference
- Cisco IOS Security Configuration Guide

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The ST and the TOE it describes are conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009
  - Part 3 Conformant

2.2 Protection Profile Conformance

This ST claims compliance to the following Common Criteria validated Protection Profiles (PP), US Government, Security Requirements for Network Devices (pp_nd_v1.0), version 1.0, dated 10 December 2010 (from here within referred to as NDPP).

2.2.1 Protection Profile Additions

The ST claims conformance to the NDPP and does not include any additions to the functionality described in the Protection Profile.

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 US Government, Security Requirements for Network Devices for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target.

2.3.3 Statement of Security Objectives 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.

2.3.4 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the U.S. Government Protection Profile for Security Requirements for Network Devices for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in the Security Target. Additionally, the Security Assurance Requirements included in the Security Target 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 7: TOE Assumptions

Assumption	Assumption Definition
Reproduced from the Security Requirements for NDPP	
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 IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Basic.

Table 8: Threats

Threat	Threat Definition
Reproduced from the Security Requirements for NDPP	
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.RESOURCE_EXHAUSTION	A process or user may deny access to TOE services by exhausting critical resources on the TOE.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
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

Threat	Threat Definition
	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

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

Table 9: Organizational Security Policies

Policy Name	Policy Definition
Reproduced from the Security Requirements for NDPP	
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 operational environment in meeting the security needs.

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

4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 10: Security Objectives for the TOE

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

TOE Objective	TOE Security Objective Definition
	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 NDPP non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 11: Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
Reproduced from the Security Requirements for NDPP	
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from *US Government, Security Requirements for Network Devices (pp_nd_v1.0), version 1.0, dated 10 December 2011*.

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: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [[***selected-assignment***]]).
- Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
- Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number placed at the end of the component. For example FDP_IFF.1(1) and FDP_IFF.1(2) indicate that the ST includes two iterations of the FDP_IFF.1 requirement, (1) and (2).
- Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- The Extended SFRs are identified by having a label '_EXT' after the requirement name for TOE SFRs.

Other sections of the ST use bolding to highlight text of special interest, such as captions.

5.2 TOE Security Functional Requirements

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

Table 12: Security Functional Requirements

Functional Component	
Requirement Class	**Requirement Component**
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_STG_EXT.1: External audit trail storage
	FAU_STG_EXT.3: Action in case of loss of audit server connectivity

Functional Component	
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_RBG_EXT.1: Cryptographic operation (random bit generation)
	FCS_COMM_PROT_EXT.1: Communications protection
	FCS_IPSEC_EXT.1: IPSEC
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.5: Password-based authentication mechanism
	FIA_UAU.6: Re-authenticating
	FIA_UAU.7: Protected authentication feedback
FMT: Security management	FMT_MTD.1: Management of TSF data (for general TSF data)
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1(1): Basic internal TSF data transfer protection (disclosure)
	FPT_ITT.1(2): Basic internal TSF data transfer protection (modification)
	FPT_PTD_EXT.1(1): Management of TSF data (for reading of authentication data)
	FPT_PTD_EXT.1(2): Management of TSF data (for reading of keys)
	FPT_RPL.1: Replay detection
	FPT_STM.1: Reliable time stamps
	FPT_TUD_EXT.1: Trusted update
	FPT_TST_EXT.1: TSF testing

Functional Component	
FRU: Resource utilization	FRU_RSA.1: Maximum quotas
FTA: TOE Access	FTA_SSL_EXT.1: TSF-initiated session locking
	FTA_SSL.3: TSF-initiated termination
	FTA_TAB.1: Default ToE access banners
FTP: Trusted path/channels	FTP_ITC.1(1): Inter-TSF trusted channel (prevention of disclosure)
	FTP_ITC.1(2): Inter-TSF trusted channel (detection of modification)
	FTP_TRP.1(1): Trusted path
	FTP_TRP.1(2): 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 basic level of audit; and

c) *All administrative actions;*

d) [*Specifically defined auditable events listed in* Table 13].

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

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

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

Table 13: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FAU_STG_EXT.3	Loss of connectivity.	No additional information.
FCS_CKM.1	Failure on invoking functionality.	No additional information.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM_EXT.4	Failure on invoking functionality.	No additional information.
FCS_COP.1(1)	Failure on invoking functionality.	No additional information.
FCS_COP.1(2)	Failure on invoking functionality.	No additional information.
FCS_COP.1(3)	Failure on invoking functionality.	No additional information.
FCS_COP.1(4)	Failure on invoking functionality.	No additional information.
FCS_RBG_EXT.1	Failure of the randomization process.	No additional information.
FCS_COMM_PROT_EXT.1	None.	
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Establishment/Termination of an IPsec SA.	Reason for failure. Non-ToE endpoint of connection (IP address) for both successes and failures.
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.5	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.6	Attempt to re-authenticate.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.1	None.	
FPT_ITT.1(1)	None.	
FPT_ITT.1(2)	None.	
FPT_PTD.1(1)	None.	
FPT_PTD.1(2)	None.	
FPT_RPL.1	Detected replay attacks.	Origin of the attempt (e.g., IP address).
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).

Requirement	Auditable Events	Additional Audit Record Contents
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”.
FRU_RSA.1	Maximum quota being exceeded.	Resource identifier.
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 the session locking mechanism.	No additional information.
FTA_TAB.1	None.	
FTP_ITC.1(1)	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_ITC.1(2)	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1(1)	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.
FTP_TRP.1(2)	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

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 over a trusted channel defined in FTP_ITC.1***].

5.2.1.4 FAU_STG_EXT.3: Action in case of loss of audit server connectivity

FAU_STG_EXT.3.1 The TSF shall [**store audit records on the TOE and attempt re-establish connection**] if the link to the external IT entity collecting the audit data generated by the ToE is not available.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1: Cryptographic key generation (for asymmetric keys)

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys **in accordance with a domain parameter generator and** [***a random number generator***] that meet the following:

a) All cases: (i.e., any of the above)

- **ANSI X9.80 (3 January 2000), "Prime Number Generation, Primality Testing, and Primality Certificates" using random integers with deterministic tests, or constructive generation methods**
- **Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 112 bits using conservative estimates.**

~~**b) Case: For domain parameters used in finite field-based key establishment schemes**~~

- ~~**NIST Special Publication 800-56A "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"**~~

c) Case: For domain parameters used in RSA-based key establishment schemes

- **NIST Special Publication 800-56B "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"**

~~**d) Case: For domain parameters used in elliptic curve-based key establishment schemes**~~

- ~~**NIST Special Publication 800-56A "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"**~~

- ~~**The TSF shall implement "NIST curves" P-256, P-384 and [Selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard")**~~

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) 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 [***no other key sizes***] that meets the following:

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

5.2.2.4 FCS_COP.1(2): Cryptographic operation (for cryptographic signature)

FCS_COP.1.1(2) The TSF shall perform **cryptographic signature services** in accordance with a [***(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater***] that meets the following:

Case: RSA Digital Signature Algorithm

- [***FIPS PUB 186-3, "Digital Signature Standard"***]

5.2.2.5 FCS_COP.1(3): Cryptographic operation (for cryptographic hashing)

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

5.2.2.7 FCS_RBG_EXT.1: Cryptographic operation (random bit generation)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [***NIST Special Publication 800-90 using***

CTR_DRBG (AES)] seeded by an entropy source that accumulated entropy from at least one independent TSF-hardware-based noise source.

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

5.2.2.8 FCS_COMM_PROT_EXT.1: Communications protection

FCS_COMM_PROT_EXT.1.1 The TSF shall protect communications using [***IPsec***] and [***no other protocol***].

5.2.2.9 FCS_IPSEC_EXT.1: IPSEC

FCS_IPSEC_EXT.1.1 The TSF shall implement IPSec using the ESP protocol as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [***no other algorithms***] and using IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109, [***no other methods***] to establish the security association.

FCS_IPSEC_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

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

FCS_IPSEC_EXT.1.4 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to [**an administratively configurable number of kilobytes including the range from 100 – 200**] MB of traffic for Phase 2 SAs.

FCS_IPSEC_EXT.1.5 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP) and [***no other DH groups***].

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

FCS_IPSEC_EXT.1.7 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its IPSec connections.

FCS_IPSEC_EXT.1.8 The TSF shall support the following:

- Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”);
- Pre-shared keys of 22 characters [***no other lengths***].

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 special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")");*
2. *Minimum password length shall be settable by the Security Administrator, and support passwords of 8 characters or greater;*
3. *Passwords composition rules specifying the types and number of required characters that comprise the password shall be settable by the Security Administrator.*
4. *Passwords shall have a maximum lifetime, configurable by the Security Administrator.*
5. *New passwords must contain a minimum of 4 character changes from the previous password.*

5.2.4.2 FIA_UIA_EXT.1: User identification and authentication

FIA_UIA_EXT.1.1 The TSF shall allow [***no services***] on behalf of the user to be performed before the user is identified and authenticated.

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

5.2.4.3 FIA_UAU_EXT.5: Password-based authentication mechanism

FIA_UAU_EXT.5.1 The TSF shall provide a local password-based authentication mechanism, [[***remote password-based authentication via RADIUS or TACACS+***]] to perform user authentication.

FIA_UAU_EXT.5.2 The TSF shall ensure that users with expired passwords are **[*required to create a new password after correctly entering the expired password*]**.

5.2.4.4 FIA_UAU.6: Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions: when the user changes their password, **[*following TSF-initiated locking (FTA_SSL), no other conditions*]**.

5.2.4.5 FIA_UAU.7: Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the 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 The TSF shall be capable of performing the following management functions:

- *Ability to configure the list of TOE services available before an entity is identified and authenticated, as specified in FIA_UAU.1, respectively.*
- *Ability to configure the cryptographic functionality.*
- *Ability to update the TOE, and to verify the updates using the digital signature capability (FCS_COP.1(2)) and* [***no other functions***].

5.2.5.3 FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

- [Security Administrator ***(also known as privileged administrator)***,
- [***semi-privileged administrator, and neighbor routers***]].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 FPT_ITT.1(1) Basic Internal TSF Data Transfer Protection (Disclosure)

5.2.6.2 FPT_ITT.1.1(1) **Refinement:** The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE **through the use of the TSF-provided cryptographic services:** [**FCS_IPSEC_EXT.1 IPSEC**].

5.2.6.3 FPT_ITT.1(2) Basic Internal TSF Data Transfer Protection (Modification)

5.2.6.4 FPT_ITT.1.1(2) **Refinement:** The TSF shall **detect modification of** TSF data when it is transmitted between separate parts of the TOE **through the use of the TSF-provided cryptographic services:** [**FCS_IPSEC_EXT.1 IPSEC**].

5.2.6.5 FPT_PTD_EXT.1(1): Management of TSF data (for reading of authentication data)

FPT_PTD_EXT.1.1(1) The TSF shall **prevent** *reading of* the *plaintext passwords*.

5.2.6.6 FPT_PTD_EXT.1(2): Management of TSF data (for reading of all symmetric keys)

FPT_PTD_EXT.1.1(2) The TSF shall **prevent** *reading of all pre-shared keys, symmetric key, and private keys*.

5.2.6.7 FPT_RPL.1: Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [*network packets terminated at the TOE*].

FPT_RPL.1.2 The TSF shall perform: [*reject the data*] when replay is detected.

5.2.6.8 FPT_STM.1: Reliable time stamps

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

5.2.6.9 FPT_TUD_EXT.1: 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 the TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [***published hash***] prior to installing those updates.

5.2.6.10 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.

5.2.7 FRU – Resource Utilization

5.2.7.1 FRU_RSA.1: Maximum quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [**resources supporting the administrative interface**], [***no other resource***] that [***individual user***] can use [***simultaneously***].

5.2.8 TOE Access (FTA)

5.2.8.1 FTA_SSL_EXT.1: TSF-initiated session locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.2.8.2 FTA_SSL.3: TSF-initiated termination

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

5.2.8.3 FTA_TAB.1: Default TOE Access Banners

FTA_TAB.1.1 Before establishing a **user/administrator** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding unauthorized use of the TOE.

5.2.9 Trusted Path/Channel (FTP)

5.2.9.1 FTP_ITC.1(1): Inter-TSF trusted channel (prevention of disclosure)

FTP_ITC.1.1(1) The TSF shall **use [IPsec] to** provide a **trusted** communication channel between itself and **authorized IT entities** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure.

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

FTP_ITC.1.3(1) The TSF shall initiate communication via the trusted channel for [*all authentication functions),* [**IPsec**]].

5.2.9.2 FTP_ITC.1(2) – Inter-TSF trusted channel (detection of modification)

FTP_ITC.1.1(2) The TSF shall **use [IPsec] in providing** a **trusted** communication channel between itself and **authorized IT entities** that is logically distinct from other communication channels and provides assured identification of its end points and **detection of the modification of data**.

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

FTP_ITC.1.3(2) The TSF shall initiate communication via the trusted channel for [*all authentication functions),* [**IPsec**]].

5.2.9.3 FTP_TRP.1(1): Trusted path

FTP_TRP.1.1(1) **Refinement:** The TSF shall provide a communication path between itself and *remote administrators* **using [IPSec as specified in FCS_IPSec_EXT.1 to access the CLI]** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure.

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

FTP_TRP.1.3(1) **Refinement:** The TSF shall require the use of the trusted path for *all remote administrative actions*.

5.2.9.4 FTP_TRP.1(2) – Trusted path

FTP_TRP.1.1(2) **Refinement:** The TSF shall provide a communication path between itself and *remote administrators* **using [IPSec as specified in FCS_IPSec_EXT.1 to access the CLI]** that is logically distinct from other communication paths and provides assured identification of its end points and **detection of modification of the communicated data**.

FTP_TRP.1.2(2) The TSF shall permit *remote administrators* to initiate communication via the trusted path.

FTP_TRP.1.3(2) **Refinement:** The TSF shall require the use of the trusted path for *all remote administrative actions*.

5.3 Extended Components Definition

This Security Target includes Security Functional Requirements (SFR) that is not drawn from existing CC Part 2. The Extended SFRs are identified by having a label '_EXT' after the requirement name for TOE SFRs. The structure of the extended SFRs is modeled after the SFRs included in CC Part 2. The structure is as follows:

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

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

C. Component – The extended SFRs are not hierarchical to any other components, though they may have identifiers terminating on other than "1". The dependencies for each extended component are identified in the TOE SFR Dependencies section of this ST below.

D. The management requirements, if any, associated with the extended SFRs are incorporated into the Security management SFRs defined in this ST.

E. The audit requirements, if any, associated with the extended SFRs are incorporated into the Security audit SFRs defined in this ST.

F. The dependency requirements, if any, associated with the extended SFRs are identified in the dependency rationale and mapping section of the ST (TOE SFR Dependencies Rationale).

Extended Requirements Rationale:

FAU_STG_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement to export audit records outside the TOE.

FAU_STG_EXT.3:

This SFR was taken from NDPP – where it is defined as a requirement to detect, and take a defined action, when an external audit server becomes inaccessible.

FCS_CKM_EXT.4:

This SFR was taken from NDPP – where it is defined as a requirement for immediate zeroization when keys and CSPs are no longer required.

FCS_COMM_PROT_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement to identify required protocol-related cryptographic mechanisms.

FCS_IPSEC_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement specific to IPSEC.

FCS_RBG_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement specific to random bit generation.

FIA_PMG_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement for specific password composition and aging constraints. Note that "Security Administrator" has been replaced with "Authorized Administrator".

FIA_UAU_EXT.5:

This SFR was taken from NDPP – where it is defined as a requirement allowing the identification of required external authentication services.

FIA_UIA_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement combining both identification and authentication requirements.

FPT_PTD_EXT.1:

This SFR was taken from NDPP (as FPT_PTD.1(1)) –where it is defined as a requirement specifically disallowing access to identified TSF data. Note, in the NDPP this SFR is not represented as an Extended Requirement with the inclusion of the 'EXT' qualifier. However this SFR is not represented in the Part 2 CC, as such the ST Author has corrected by including the 'EXT' qualifier.

FPT_PTD_EXT.2:

This SFR was taken from NDPP (as FPT_PTD.1(2)) – where it is defined as a requirement specifically disallowing access to identified TSF data. Note, in the NDPP this SFR is not represented as an Extended Requirement with the inclusion of the 'EXT' qualifier. However this SFR is not represented in the Part 2 CC, as such the ST Author has corrected by including the 'EXT' qualifier.

FPT_TST_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement for TSF self tests of the TOE during initialization (on bootup).

FPT_TUD_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement for secure TOE update capabilities. Note that

"Security Administrator" has been replaced with "Authorized Administrator".

FTA_SSL_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement for behavior after local terminal session inactivity. Note that "Security Administrator" has been replaced with "Authorized Administrator".

5.4 TOE SFR Dependencies Rationale

The following table provides dependency rational for SFRs that were drawn from the NDPP.

Table 14: SFR Dependency Rationale (from NDPP)

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Met by FAU_GEN. Met by FIA_UIA_EXT.1
FAU_STG_EXT.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_STG_EXT.3	FAU_STG_EXT.1	Met by FAU_STG_EXT.1
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Met by FCS_COP.1(2), (3), and (4) Met by FCS_CKM.4
FCS_CKM_EXT.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Met by FCS_CKM.1(1), (2)
FCS_COP.1(1)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Met by FCS_CKM.1(1), (2) and FCS_CKM_EXT.4
FCS_COP.1(2)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Met by FCS_CKM.1(1), (2) and Met by FCS_CKM_EXT.4
FCS_COP.1(3)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Met by FCS_CKM.1(1), (2) and Met by FCS_CKM_EXT.4
FCS_COP.1(4)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Met by FCS_CKM.1(1), (2) and Met by FCS_CKM_EXT.4
FCS_RBG_EXT.1	No dependencies	N/A
FCS_COMM_PROT_EXT.1	FCS_HTTPS_EXT.1 or FCS_IPSEC_EXT.1 or FCS_SSH_EXT.1 or FCS_TLS_EXT.1	Met by FCS_IPSEC_EXT.1
FCS_IPSEC_EXT.1	FCS_COP.1	Met by FCS_COP.1

SFR	Dependency	Rationale
FDP_RIP.2	No dependencies	N/A
FIA_PMG_EXT.1	No dependencies	N/A
FIA_UIA_EXT.1	No dependencies	N/A
FIA_UAU_EXT.5	No dependencies	N/A
FIA_UAU.6	No dependencies	N/A
FIA_UAU.7	FIA_UAU.1	Met by FIA_UIA_EXT.1
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Met by FMT_SMF.1 Met by FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	Met by FIA_UIA_EXT.1
FPT_ITT.1(1)	No dependencies	N/A
FPT_ITT.1(2)	No dependencies	N/A
FPT_PTD_EXT.1(1)	No dependencies	N/A
FPT_PTD_EXT.1(2)	No dependencies	N/A
FPT_RPL.1	No dependencies	N/A
FPT_STM.1	No dependencies	N/A
FPT_TUD_EXT.1	No dependencies	N/A
FPT_TST_EXT.1	No dependencies	N/A
FRU_RSA.1	No dependencies	N/A
FTA_SSL_EXT.1	No dependencies	N/A
FTA_SSL.3	No dependencies	N/A
FTA_TAB.1	No dependencies	N/A
FTP_ITC.1(1)	No dependencies	N/A
FTP_ITC.1(2)	No dependencies	N/A
FTP_TRP.1(1)	No dependencies	N/A
FTP_TRP.1(2)	No dependencies	N/A

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDPP which are derived from Common Criteria Version 3.1, Revision 3. The assurance requirements are summarized in the table below as identified in the NDPP, Section 4.3. The ST does not include any changes to the assurance requirements beyond those identified and described in the NDPP.

Table 15: 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 Security Target claims conformance to the NDPP which draws from EAL1 the Security Assurance Requirements (SARs). 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.

5.6 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 16: 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.

Component	How requirement will be met
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s) identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ALC_CMS.1	
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

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

Table 17: How TOE SFRs are met

TOE SFRs	How the SFR is Met
FAU_GEN.1	The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table"). Each of the events is specified in the audit record is in enough detail to identify the user for which the event is associated (e.g. user identity, MAC address, IP address), when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited. The audit trail consist of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. As noted above, the information includes [at least] all of the required information. Additional information can be configured and included if desired. Refer to the Guidance documentation in Section 1.9 for configuration syntax and information. The logging buffer size can be configured from a range of 4096 (default) to 2147483647 bytes. It is noted, not make the buffer size too large because the switch could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should not be set to this amount. Refer to the Guidance documentation in Section 1.9 for configuration syntax and information. The administrator can also configure a 'configuration logger' to keep track of configuration changes made with the command-line interface (CLI). The administrator can configure the size of the configuration log from 1 to 1000 entries (the default is 100). Refer to the Guidance documentation in Section 1.9 for configuration syntax and information. The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc.; all of which are described in the Guidance documents and IOS CLI. Refer to the Guidance documentation in Section 1.9 for configuration syntax and information The logs can be saved to flash memory so records are not lost in case of failures or restarts. Refer to the Guidance documentation in Section 1.9 for configuration syntax and information.

The administrator can set the level of the audit records to be displayed on the console or sent to the syslog server. For instance all emergency, alerts, critical, errors, and warning message can be sent to the console alerting the administrator that some action needs to be taken as these types of messages mean that the functionality of the switch is affected. All notifications and information type message can be sent to the syslog server, whereas message is only for information; switch functionality is not affected.

To configure the TOE to send audit records to a syslog server, the 'set logging server' command is used. A maximum of three syslog servers can be configured. Refer to the Guidance documentation in Section 1.9 for configuration syntax and information. The audit records are transmitted using IPsec tunnel to the syslog server. If the communications to the syslog server is lost, the TOE generates an audit record and all permit traffic is denied until the communications is re-established.

The FIPS crypto tests performed during startup, the messages are displayed only on the console. Once the box is up and operational and the crypto self-test command is entered, then the messages would be displayed on the console and will also be logged.
For the TSF self-test, successful completion of the self-test is indicated by reaching the log-on prompt. If there are issues, the applicable audit record is generated and displayed on the console.

The following table identifies the required auditable events, the rationale for generating the record and any additional information that is required beyond the default information listed in FAU_GEN.1.2.

Auditable Event	**Rationale**
All use of the user identification and authentication mechanism.	Events will be generated for attempted identification/ authentication, and the username attempting to authenticate and the origin of the attempt will be included in the log record.
All use of the authentication mechanism and attempt to re-authenticate	Events will be generated for attempted authentication and attempt to re-authenticate, the username attempting to authenticate will be included in the log record, along with the origin or source of the attempt.
Failure on invoking cryptographic functionality to include, asymmetric key generation, key zeroization, cryptographic signature, cryptographic hashing, keyed-hash message authentication and Random Bit Generation	The audit record will include the default required information for each of the failures when triggered, no additional required

	Detection of replay attacks	Attempts of replaying data previously transmitted and terminated at the TOE are logged, along with the origin or source of the attempt.	
	Changes to the time.	Changes to the time are logged; including the old and new values for the time along with the origin of the attempt	
	Updates	An audit record will be generated on the initiation of updates (software/firmware)	
	Failure to establish and/or establishment/failure of an IPsec session	Attempts to establish an IPsec session or the failure of an established IPsec is logged.	
	Resources quotas are exceeded	If the threshold for the number of concurrent administrative sessions is exceeded, an audit record is generated with the resource identifier included in the record	
	Attempts at unlocking interactive sessions	Any attempt to unlock an inactive sessions is logged, as	
	Termination of a remote session by locking the session	When a session is locked, the session is terminated, thus generating an audit record	
	Indication that TSF self-test was completed.	During bootup, if the self test fails, the failure is logged.	
	Trusted channels	The initiation, termination, and failure related to trusted channel sessions with the remote administration console, syslof server, remote authentication server and if connected the NTP server. The initiator and the target of the trusted channel is identified and included in the audit record.	
FAU_GEN.2	The TOE shall ensure that each auditable event is associated with the user 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, MAC address, host name, or other configured identification is presented. Refer to the Guidance documentation in Section 1.9 for configuration syntax and information.		
FAU_STG_EXT. 1 and	The TOE is configured to export syslog records to a specified, external syslog server. The TOE protects communications with an external syslog server via		

<table>
<tr><td>FAU_STG_EXT.3</td><td>IPsec. If the IPsec connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server.

For audit records stored internally to the TOE, the administrator has the ability to configure the TOE to stop all auditable events when an audit storage threshold is met (lossless auditing) or given the log file is circular, the TOE may overwrite the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 4096 (default) to 2147483647 bytes of available disk space. Refer to the Guidance documentation in Section 1.9 for configuration syntax and information.</td></tr>
<tr><td>FCS_CKM.1</td><td>The TOE implements a random number generator for RSA key establishment schemes (conformant to NIST SP 800-56B. The TOE is also compliant to ANSI X9.80 (3 January 2000), “Prime Number Generation, Primality Testing, and Primality Certificates” using random integers with deterministic tests. Furthermore, the TOE does not implement elliptic-curve-based key establishment schemes.</td></tr>
<tr><td>FCS_CKM_EXT.4</td><td>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. This requirement applies to the secret keys used for symmetric encryption, private keys, and CSPs used to generate key (list them); which are zeroized immediately after use, or on system shutdown, etc.
<table>
<tr><th>Name</th><th>Description of Key</th><th>Storage</th><th>Zeroization</th></tr>
<tr><td>Diffie-Hellman Shared Secret</td><td>This is the shared secret used as part of the Diffie-Hellman key exchange.</td><td>SDRAM (plaintext)</td><td>Automatically after completion of DH exchange.

Overwritten with: 0x00</td></tr>
<tr><td>Diffie Hellman private exponent</td><td>This is the private exponent used as part of the Diffie-Hellman key exchange.</td><td>SDRAM (plaintext)</td><td>Zeroized upon completion of DH exchange.

Overwritten with: 0x00</td></tr>
<tr><td>Skeyid</td><td>This is an IKE intermitent value used to create skeyid_d.</td><td>SDRAM (plaintext)</td><td>Automatically after IKE session terminated.</td></tr>
</table>
</td></tr>
</table>

					Overwritten with: 0x00	
		skeyid_d	This is an IKE intermitent value used to derive keying data for IPsec.	SDRAM (plaintext)	Automatically after IKE session terminated. Overwritten with: 0x00	
		IKE session encrypt key	This the key IPsec key used for encrypting the traffic in an IPsec connection.	SDRAM (plaintext)	Automatically after IKE session terminated. Overwritten with: 0x00	
		IKE session authentication key	This the key IPsec key used for authenticating the traffic in an IPsec connection.	SDRAM (plaintext)	Automatically after IKE session terminated. Overwritten with: 0x00	
		ISAKMP preshared	This is the configured pre-shared key for ISAKMP negotiation.	NVRAM (plaintext)	Zeroized using the following command: **# no crypto isakmp key** Overwritten with: 0x0d	
		IKE RSA Private Key	The RSA private-public key pair is created by the device itself using the key generation CLI described below. Afterwards, the device's public key must be put into the	NVRAM (plaintext)	Zeroized using the following command: **# crypto key zeroize rsa** Overwritten with: 0x0d	

			device certificate. The device's certificate is created by creating a trustpoint on the device. This trustpoint authenticates with the CA server to get the CA certificate and also enrolls with the CA server to generate the device certificate. In the IKE authentication step, the device's certificate is firstly sent to other device to be authenticated. The other device verifies that the certificate is signed by CA's signing key, then sents back a random secret encrypted by the device's public key in the valid device certificate. . Only the device with the matching device private key can decrypt the message and obtain the			

			random secret.			
		IPsec encryption key	This is the key used to encrypt IPsec sessions.	SDRAM (plaintext)	Automatically when IPsec session terminated. Overwritten with: 0x00	
		IPsec authentication key	This is the key used to authenticate IPsec sessions.	SDRAM (plaintext)	Automatically when IPsec session terminated. Overwritten with: 0x00	
		RADIUS secret	Shared secret used as part of the Radius authentication method.	NVRAM (plaintext)	Zeroized using the following command: **# no radius-server key** Overwritten with: 0x0d	
		TACACS+ secret	Shared secret used as part of the TACACS+ authentication method.	NVRAM (plaintext)	Zeroized using the following command: **# no tacacs-server key** Overwritten with: 0x0d	
FCS_COP.1(1)	The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128, 256 bits) as described in FIPS PUB 197, NIST SP 800-38A and NIST SP 800-38D.					
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".
FCS_COP.1(3)	The TOE provides cryptographic hashing services using SHA-1, SHA-256, and SHA-512 as specified in FIPS Pub 180-3 "Secure Hash Standard." Please see CAVP certificate # 1940, Rel 1.0.0 for validation details.
FCS_COP.1(4)	The TOE uses HMAC-SHA1 message authentication as part of the RADIUS Key Wrap functionality as specified in FIPS Pub 198-1 "The Keyed-Hash Message Authentication Code" and FIPS PUB 180-3, "Secure Hash Standard". Please see CAVP certificate # 1940 Rel 1.0.0 for validation details.
FCS_RBG_EXT.1	The TOE (Cisco Catalyst Switches (3560C, 3560X and 3750X) running IOS 15.0(2)SE4); hence the product implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90. The entropy source used to seed the Deterministic Random Bit Generator (e.g. based on SP 800-90A/B/C) is a random set of bits or bytes that are regularly supplied to the DRBG from the internal Quack (ACT) processor which produces a minimum of 256 bits of entropy This solution is available in the 15.0(2)SE1/SE2/SE4 or later FIPS/CC approved releases of the IOS images relating to the platforms mentioned above. All RNG entropy source samplings are continuously health tested by the NIST DRBG as per SP 900-90A before using them as a seed. Though related to this, the tests are part of the FIPS validation procedures for the DBRG and are part of the NIST validations for FIPS 140-2 for the products. Any initialization or system errors during bring-up or processing of this system causes a reboot as necessary to be FIPS compliant. Finally, the system will be zeroizing any entropy seeding bytes, which will not be available after the current collection.
FCS_COMM_PROT_EXT.1	The TOE implements IPsec that is used to protect communications for remote administration. IPsec is also used to protect communications with external servers (e.g., syslog server, NTP, and if configured external authentication servers).
FCS_IPSEC_EXT.1	The TOE implements IPsec to provide authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE implementation of the IPsec standard (in accordance with the RFCs noted in the SFR) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services. IPsec Internet Key Exchange, also called ISAKMP, is the negotiation protocol that lets two peers agree on how to build an IPsec Security Association (SA). The IKE protocols implement Peer Authentication using the rDSA algorithm. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including: • The negotiation of mutually acceptable IPsec options between peers, • The establishment of additional Security Associations to protect

	packets flows using ESP, and • The agreement of secure bulk data encryption AES (128 and 256 bit) keys for use with ESP. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation. The TOE supports IKEv1 session establishment. As part of this support, the TOE can be configured to not support aggressive mode for IKEv1 exchanges and to only use main mode using the 'crypto isakmp aggressive-mode disable' command as specified for the evaluated configuration. The TOE can be configured to not allow "confidentiality only" ESP mode by ensuring the IKE Policies configured include ESP-encryption. The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using "lifetime" command. The default time value for Phase 1 SAs is 24 hours. The default time value for Phase 2 SAs is 1 hour, but it is configurable to 8 hours. The TOE also supports configuration of maximum traffic that is allowed to flow for a given IPsec SA using the following command, 'crypto ipsec security-association lifetime' as specified for the evaluated configuration. The default amount is 2560KB, which is the minimum configurable value. The maximum configurable value is 4GB. However, the TOE is to be configured to use a range between 100-200 MB as specified in the SFR. Other configuration options include rDSA algorithm for implementing peer authentication as noted above, pre-shared keys for authenticating IPsec connections can be 22 characters and be composed of any combination of upper and lower case letters, numbers, and special characters using the 'crypto isakmp key' key command and may be proposed by each of the peers negotiating the IKE establishment. The TOE also supports both rekey and response to rekeyed by the peer for phase 2 (IPsec) SA The TOE also supports Diffie-Hellman Group 14 (2048-bit keys) in support of IKE Key Establishment
FDP_RIP.2	The TOE ensures that packets transmitted from the TOE do not contain residual information from previous packets. Packets that are not the required length use zeros for padding. Residual data is never transmitted from the TOE. Once packet handling is completed its content is overwritten before memory buffer which previously contained the packet is reused. This applies to both data plane traffic and administrative session traffic.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". Minimum password length is settable by the Authorized Administrator, and support passwords of 8 characters or greater. Password composition rules specifying the types and number of required characters that comprise the password are settable by the Authorized Administrator. Passwords have a maximum lifetime, configurable by the Authorized Administrator. New passwords must contain a minimum of 4 character changes from the previous password.
FIA_UIA_EXT.1	The TOE requires all users to be successfully identified and authenticated before allowing any services and/or TSF mediated actions to be performed per

	the authentication policy.
FIA_UAU_EXT.5	The TOE can be configured to require local authentication and/or remote authentication via a RADIUS or TACACS+ server as defined in the authentication policy for interactive (human) users. Neighbor routers are authenticated only to passwords stored locally. The policy for interactive (human) users (Administrators) can be authenticated to the local user database, or have redirection to a remote authentication server. Interfaces can be configured to try one or more remote authentication servers, and then fail back to the local user database if the remote authentication servers are inaccessible. If the interactive (human) users (Administrators) password is expired, the user is required to create a new password after correctly entering the expired password.
FIA_UAU.6	Users changing their passwords due to password expiration are first prompted to enter their old password and then choosing a new password (that meets the password complexity requirements). Users are also required to enter their password when re-establishing a remote session due to a lock out of inactivity. The TOE does not provide the capability for an administrator (level 1) to change their own password. However the administrator (level 1) can change their password when required by the TOE (e.g. when expired). At which time the administrator is required to enter their current password before entering a new password. System administrators (level 15) can change any user's password, including their own as required for TOE management, though must be in privilege EXEC mode to perform the function. When the System Administrator (level 15) attempts to change their own password, the TOE will enforce the password expiration policy at which time the System Administrator (level 15) will be required to enter their current password prior to entering a new password. See the Installation and Configuration for Common Criteria NDPP V1.0 Evaluated Cisco IOS Catalyst Switches (3560C, 3560-X and 3750-X) for details and configuration settings.
FIA_UAU.7	When a user enters their password at the local console, the console only displays '*' characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.
FMT_MTD.1	The TOE provides the ability for authorized administrators to access TOE data, such as audit data, configuration data, security attributes, and session thresholds. Each of the predefined and administratively configured roles has create (set), query, modify, or delete access to the TOE data. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15; and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. The term "authorized administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. Therefore, semi-privileged

	administrators with only a subset of privileges can also modify TOE data based if granted the privilege.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The administrative user can connect to the TOE using the CLI to perform these functions via SSHv2 through an IPsec encrypted session, a terminal server, or at the local console. Refer to the Guidance documentation in Section 1.9 for configuration syntax and information related to each of these functions. Note, the Common Criteria certification did not evaluate SSH functionality. The management functionality provided by the TOE include the following administrative functions: • Ability to manage the cryptographic functionality - allows the authorized administrator the ability to identify and configure the algorithms used to provide protection of the data, configuration of routing protocols, and if used the configuration of remote authentication • • Ability to update the TOE and verify the updates are valid.
FMT_SMR.1	The TOE switch platform maintains administrative privilege level The term "authorized administrator" is used in this ST to refer to any user that has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. The Switch can and shall be configured to authenticate all access to the command line interface using a username and password.
FPT_ITT.1(1) and FPT_ITT.1(2)	The TOE is not a distributed product. The TOE is self-contained and provides all of the claimed functionality within a single appliance.
FPT_PTD_EXT.1 and FPT_PTD_EXT.2	The TOE includes CLI command features that can be used to configure the TOE to encrypt all locally defined user passwords. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. The command is the *password encryption aes* command used in global configuration mode. The command *service password-encryption* applies encryption to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords. Refer to Cisco Catalyst 3560C, 3560X and 3750X Switches Common Criteria Operational User Guidance and Preparative Procedures for command description and usage. The TOE stores all private keys in a secure directory that is not readily accessible to administrators; hence no interface access. Additional, all pre-shared and symmetric keys are stored in encrypted form to prevent access.
FPT_RPL.1	By virtue of the cryptographic and path mechanisms implemented by the TOE, replayed network packets directed (terminated) at the TOE will be detected

	and discarded. Note: The intended scope of this requirement is trusted communications with the TOE (e.g., administrator to TOE, IT entity (e.g., authentication server) to TOE). As such, replay does not apply to receipt of multiple network packets due to network congestion or lost packet acknowledgments.
FPT_STM.1	The TOE provides a source of date and time information for the switch, used in audit timestamps and in validating service requests. This function can only be accessed from within the configuration exec mode via the privileged mode of operation of the switch. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive time from an NTP server. If an NTP server is used, the TOE supports signature verification of the timestamp from the time server.
FPT_TUD_EXT.1	The TOE has specific versions that can be queried by an administrator. When updates are made available by Cisco, an administrator can obtain and install those updates. The cryptographic checksums (i.e., public hashes) are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components.
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. If any of the tests fail, the security administrator will have to log into the CLI to determine which test failed and why. If the tests pass successfully the login prompt is displayed. Refer to the FIPS Security Policy for available options and management of the cryptographic self-test. In addition to the FIPS self-test, the administrator can also issue the command, *test crypto self-test* which test the crypto configuration. The results will generate a log file that will display a SELF_TEST_RESULT or a SELF_TEST_FAILURE. Below is a sample result file that shows the tests that are run: Router# test crypto self-test *Apr 23 01:48:49.678: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test ac) *Apr 23 01:48:49.822: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DH self test) *Apr 23 01:48:49.954: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software Cry) *Apr 23 01:48:50.054: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software che) *Apr 23 01:48:50.154: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DES encrypti) Router# *Apr 23 01:48:50.254: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (3DES encrypt) *Apr 23 01:48:50.354: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA hashing) *Apr 23 01:48:50.454: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Random KAT t) *Apr 23 01:48:50.674: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (AES encrypti) *Apr 23 01:48:50.774: %CRYPTO-6-SELF_TEST_RESULT: Self test info:

	(HMAC-SHA) Router# *Apr 23 01:48:50.874: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA256 hashi) *Apr 23 01:48:50.974: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA512 hashi) *Apr 23 01:48:50.974: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (ALL TESTS PA) For testing of the TSF, the TOE automatically runs checks and tests at startup and during resets to ensure the TOE hardware and software components are available and operating correctly. If all components pass the tests, the login prompt will be displayed. If any of the tests fail, the TOE will reboot to try to correct the issue(s). The switch LEDs provide troubleshooting information about the switch. They show POST failures, port-connectivity problems, and overall switch performance. When the switch begins POST, the Status LED turns green. The System LED blinks green, and the other LEDs stay green. When POST completes successfully, the System LED remains green. The XPS LED is green for some time and then returns to its operating status. The other LEDs turn off and return to their operating status. If the switch fails POST, the System and Ethernet management port LEDs turn amber. The various LEDs monitor a specific component and/or activity that indicate the health or failure of that feature. Refer to the Guidance documentation in Section 1.9 for installation configuration settings and information and troubling shooting if issues are identified, specifically the Hardware Installation Guide.
FRU_RSA.1	An administrator can configure a maximum number of concurrent sessions for remote administrative interfaces.
FTA_SSL_EXT.1 and FTA_SSL.3	An administrator can configure maximum inactivity times for both local and remote administrative sessions. When a session is inactive (i.e., not session input) for the configured period of time the TOE will terminate the session, flush the screen, and no further activity is allowed requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session. The allowable range is from 1 to 65535 seconds.
FTA_TAB.1	The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.
FTP_ITC.1(1) and FTP_ITC.(2)	The TOE protects communications with authorized IT entities with IPsec. This protects the data from disclosure by encryption and by checksums that verify that data has not been modified.
FTP_TRP.1(1) and FTP_TRP.1(2)	All remote administrative communications take place over a secure encrypted IPsec session. The remote users are able to initiate IPsec communications with the TOE.

6.2 TOE Bypass and interference/logical tampering Protection Measures

The TOE consists of a hardware platform in which all operations in the TOE scope are protected from interference and tampering by untrusted subjects. All administration and configuration

operations are performed within the physical boundary of the TOE. Also, all TSP enforcement functions must be invoked and succeed prior to functions within the TSC proceeding.

The TOE has been designed so that all locally maintained TSF data can only be manipulated via the secured management interface, the 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 and 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.

The TOE enforces information flow control policies and applies network traffic security on its interfaces before traffic passes into or out of the TOE. The TOE controls every ingress and egress traffic flow. Policies are applied to each traffic flow. Traffic flows characterized as unauthorized are discarded and not permitted to circumvent the TOE. There are no unmediated traffic flows into or out of the TOE. The information flow policies are applied to all traffic received and sent by the TOE. Each communication including data plane communication, control plane communications, and administrative communications are mediated by the TOE. The data plane allows the ability to forward network traffic; the control plane allows the ability to route traffic correctly; and the management plane allows the ability to manage network elements. There is no opportunity for unaccounted traffic flows to flow into or out of the TOE.

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 RATIONALE

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined within this Security Target. The following matrix is the typical display that is drawn from the information presented in Sections 2 and 3 of the NDPP. The threats and objectives that are in addition to those in the NDPP are also included in the matrix.

7.1 Rationale for TOE Security Objectives

Table 18: Threat/Objectives/Policies Mappings

	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.ADMIN_ERROR	T.UNDETECTED_ACTIONS	T.RESOURCE_EXHAUSTION	T.USER_DATA_REUSE	T.TSF_FAILURE	P.ACCESS BANNER
O.PROTECTED_COMMUNICATIONS	X	X						
O.VERIFIABLE_UPDATES		X						
O.SYSTEM_MONITORING				X				
O.DISPLAY_BANNER								X
O.TOE_ADMINISTRATION			X					
O.RESIDUAL_INFORMATION_CLEARING						X		
O.RESOURCE_AVAILABILITY					X			
O.SESSION_LOCK	X							
O.TSF_SELF_TEST							X	

Table 19: Threat/Policies/TOE Objectives Rationale

Objective	Rationale
Security Objectives Drawn from NDPP	
O.PROTECTED_COMMUNICATIONS	This security objective is necessary to counter the threats associated with secure communications, such as protected communication channels for administrators, other parts of a distributed TOE and authorized entities to ensure the communications with the TOE is not compromised
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,

Objective	Rationale
	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.

7.2 Rationale for the Security Objectives for the Environment

Table 20: Assumptions/Environment Objectives Mappings

	OE.NO_GENERAL_PURPOSE	OE.PHYSICAL	OE.TRUSTED_ADMIN
A.NO_GENERAL_PURPOSE	X		
A.PHYSICAL		X	
A.TRUSTED_ADMIN			X

Table 21: Assumptions/Threats/Objectives Rationale

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

7.3 Rationale for requirements/TOE Objectives

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

Table 22: Security Objective to Security Requirements Mappings

	O.PROTECTED_COMMUNICATIONS	O.VERIFIABLE_UPDATES	O.SYSTEM_MONITORING	O.DISPLAY_BANNER	O.TOE_ADMINISTRATION	O.RESIDUAL_INFORMATION_CLEARING	O.RESOURCE_AVAILABILITY	O.SESSION_LOCK	O.TSF_SELF_TEST
FAU_GEN.1			X						
FAU_GEN.2			X						
FAU_STG_EXT.1			X						
FAU_STG_EXT.3	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_RBG_EXT.1	X								
FCS_COMM_PROT_EXT.1	X								
FCS_IPSEC_EXT.1	X								
FCS_HTTPS_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.5					X				
FIA_UAU.6					X				
FIA_UAU.7					X				
FMT_MTD.1					X				
FMT_SMF.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_SMR.1					X				
FPT_ITT.1(1)	X								
FPT_ITT.1(2)	X								
FPT_PTD_EXT.1(1)	X				X				
FPT_PTD_EXT.1(2)	X				X				
FPT_RPL.1	X								
FPT_STM.1			X						
FPT_TUD_EXT.1		X							
FPT_TST_EXT.1									X
FRU_RSA.1							X		
FTA_SSL_EXT.1					X			X	
FTA_SSL.3					X			X	
FTA_TAB.1				X					
FTP_ITC.1(1)	X								
FTP_ITC.1(2)	X								
FTP_TRP.1(1)	X								
FTP_TRP.1(2)	X								

Table 23: Objectives to Requirements Rationale

Objective	Rationale
Security Functional Requirements Drawn from Security Requirements for NDPP	
O.PROTECTED_COMMUNICATIONS	The SFRs, FAU_STG_EXT.3, FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1, FCS_COMM_PROT_EXT.1, FCS_IPSEC_EXT.1,

Objective	Rationale
	FPT_ITT.1(1), FPT_ITT.1(2), FPT_PTD.1(1), FPT_PTD.1(2), FPT_RPL.1, FTP_ITC.1(1), FTP_ITC.1(2), FTP_TRP.1(1), FTP_TRP.1(2) meet this objective by ensuring the communications between the TOE and endpoints are secure by implementing the encryption protocols as defined in the SFRs and as specified by the RFCs.
O.VERIFIABLE_UPDATES	The SFRs, FPT_TUD_EXT.1, FCS_COP.1(2), FCS_COP.1(3) meet this objective by ensuring the update was downloaded via secure communications, is from a trusted source, and the update can be verified by cryptographic mechanisms prior to installation.
O.SYSTEM_MONITORING	The SFRs, FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1, FAU_STG_EXT.3, FPT_STM.1 meet this objective by auditing actions on the TOE. The audit records identify the user associated with the action/event, whether the action/event was successful or failed, the type of action/event, and the date/time the action/event occurred. The audit logs are transmitted securely to a remote syslog server. If connectivity to the remote syslog server is lost, the TOE will block new permit actions.
O.DISPLAY_BANNER	The SFR, FTA_TAB.1 meets this objective by displaying a advisory notice and consent warning message regarding unauthorized use of the TOE.
O.TOE_ADMINISTRATION	The SFRs, FIA_UIA_EXT.1, FIA_UAU_EXT.5, FIA_UAU.6, FIA_UAU.7, FMT_MTD.1, FMT_SMF.1, FMT_SFR.1, FPT_PTD.1(1), FTA_SSL_EXT.1, FTA_SSL.3 meet this objective by ensuring the TOE supports a password-based authentication mechanism with password complexity enforcement such as, strong passwords, password life-time constraints, providing current password when changing the password, obscured password feedback when logging in, and passwords are not stored in plaintext.
O.RESIDUAL_INFORMATION_CLEARING	The SFR, FDP_RIP.2 meets this objective by ensuring no left over user data from the previous transmission is included in the network traffic.
O.RESOURCE_AVAILABILITY	The SFR, FRU_RSA.1 meets this objective by limiting the number of amount of exhaustible resources, such the number of concurrent administrative sessions.
O.SESSION_LOCK	The SFRs, FTA_SSL_EXT.1, FTA_SSL.3 meet this

Objective	Rationale
	objective by terminating a session due to meeting/exceeding the inactivity time limit.
O.TSF_SELF_TEST	The SFR, FPT_TST_EXT.1 meets this objective by performing self-test to ensure the TOE is operating correctly and all functions are available and enforced.

ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 24: References

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, version 3.1, Revision 3
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated July 2009, version 3.1, Revision 3
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated July 2009, version 3.1, Revision 3
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated July 2009, version 3.1, Revision 3
[NDPP]	US Government, Security Requirements for Network Devices (pp_nd_v1.0), version 1.0, dated 10 December 2011