Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, 4500X) Security Target

Revision 0.098

27 November 2012

Table of Contents

List of Tables

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 (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) running IOS XE 3.3.1SG (IOS 15.1(1)SG1). 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.

REVISION HISTORY

Rev	Date	Description
0.01	12 October 2011	Initial Draft
0.02	20 October 2011	Updated based on ETR findings
0.03	25 October 2011	Updated based on ETR findings
0.04	4 November 2011	Updated based on ETR findings
0.05	15 November 2011	Updated based on ETR findings
0.06	16 March 2012	Updated based on Validator comments and additional platforms
0.07	24 April 2012	Removal of Sup6 cards and supporting platforms
0.075	25 April 2012	Added 3DES and Admin levels details
0.08	28 Mat 2012	Updated based on ETR findings
0.085	19 June 2012	Updated based on Evaluator comments
0.090	17 August 2012	Updated based on ETR Findings
0.091	23 August 2012	Updated based on ETR Findings
0.092	19 September 2012	Updated based on ETR Findings
0.093	28 September 2012	Updated based on iVOR Findings
0.094	3 October 2012	Updated based on additional findings
0.095	11 October 2012	Updated based on tVOR findings
0.096	26 October 2012	Updated based on Evaluator testing and comments
0.097	29 October 2012	Update based on Evaluator comment
0.098	27 November 2012	Update based on Validator comments

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 (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) Security Target
ST Version	0.098
Publication Date	27 November 2012
ST Author	Cisco Systems, Inc.
Developer of the TOE	Cisco Systems, Inc.
TOE Reference	Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X)
TOE Hardware Models	Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X)
TOE Software Version	IOS XE 3.3.1SG (IOS 15.1(1)SG1)
ST Evaluation Status	In Evaluation
Keywords	Audit, Authentication, Encryption, Information Flow, 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
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface

Acronyms / Abbreviations	Definition
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
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.
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 it’s 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
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 (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, and 4510R-E, and 4500X) running IOS XE 3.3.1SG (a.k.a IOS 15.1(1)SG1) (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.

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, RIPv2, and OSPFv2. BGPv4, EIGRP, and EIGRPv6 supports routing updates with IPv6 or IPv4, while RIPv2 and OSPFv2 routing protocol support routing updates for IPv4 only.

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	No	The authentication server (RADIUS and TACACS+) provides central authentication for user authorized to use the TOE. The TOE correctly leverages the services provided by the authentication server.
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Syslog server	No	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.
NTP Server	No	The TOE supports communications with an NTP server to synchronize time.

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:

- 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 slot, used to connect USB devices to the TOE (not relevant as none of the USB devices are included in the TOE)
- 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
- 10 Gigabit Ethernet (GE) uplinks and supports Power over Ethernet Plus (PoE+) and Universal POEP (UPOE). (Universal POEP is an enhancement to the PoEP (802.3at) standard to allow powered devices up to 60W to connect over a single Cat 5e cable. Standard PoEP uses only 2 twisted pairs (out of 4) in the Ethernet cable. UPOE uses all 4 twisted pairs to deliver 60W to the port.)
- Redundant power supplies and fans

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 Evaluated Configuration

The TOE consists of one or more physical devices; the Catalyst Switch with Cisco IOS XE software. The Catalyst Switch has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS 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, RIPv2, and OSPFv2 Routing protocols are used on all of the Catalyst Switch models.

The Catalyst Switch E-Series chassis come in four different form factors: 3-slot (4503-E), 6-slot (4506-E), 7-slot (4507R+E/4507R-E), and 10-slot (4510R+E/4510R-E). 4503-E, 4506-E, 4507R+E, and 4510R+E chassis are extremely flexible and support 6 Gbps, 24 Gbps, or 48Gbps per line-card slot. 4507R-E and 4510R-E chassis are limited to 6 Gbps and 24 Gbps per line-card slot. Integrated resiliency in the Cisco Catalyst 4500E Series includes 1+1 supervisor engine redundancy (10-slot and 7-slot only), redundant fans, software-based fault tolerance, and 1+1 power supply redundancy. This integrated resiliency in both hardware and software minimizes network downtime[1].

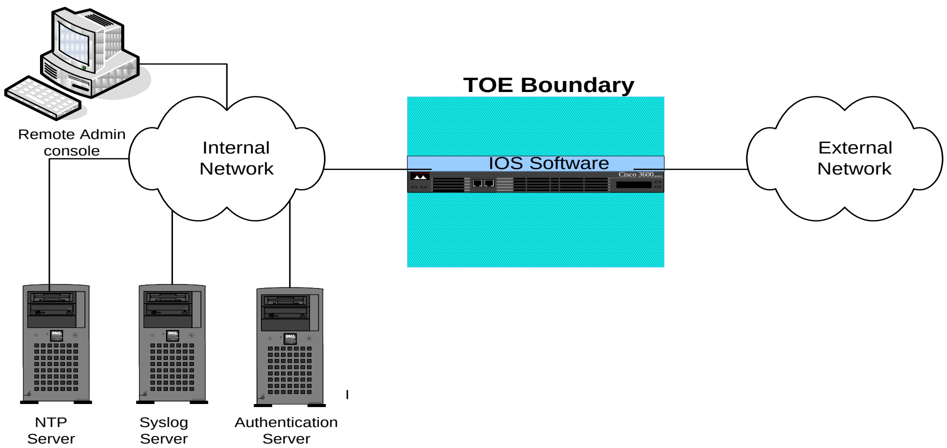
The Catalyst Switch 4500-X series is a fixed aggregation switch that provides services for space-constrained environments.

The TOE can optionally connect to an NTP server on its internal network for time services. In addition, if the Catalyst Switch is to be remotely administered, then the management station must be connected to an internal network, SSHv2 must be used to

[1] Fault tolerance is not being claimed, as all features are not supported on all models.

connect to the switch. A syslog server can also be used to store audit records. 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.



1.6 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the following switch models; Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) running IOS XE 3.3.1SG (IOS 15.1(1)SG1). The following tables further identify the supported configurations. The network, on which they reside, is part of the environment.

The Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, and 4510R-E) offers four chassis options and four supervisor engine options, however only the Supervisor 7-E and Supervisor 7L-Eare included in the evaluated configuration.

Cisco Catalyst 4503-E Cisco Catalyst 4507R+E Cisco Catalyst 4510R+E Cisco Catalyst 4506-E

Feature	Cisco Catalyst WS-C4503-E Chassis	Cisco Catalyst WS-C4506-E Chassis	Cisco Catalyst WS-C4507R+E Chassis	Cisco Catalyst WS-C4510R+E Chassis
Total number of slots	3	6	7	10
Line-card slots	2	5	5	8
Supervisor engine slots	1[2]	1	2[3]	2[4]
Dedicated supervisor engine slot numbers	1	1	3 and 4	5 and 6
Supervisor engine redundancy	No	No	Yes	Yes (Supervisor V-10GE, 6-E and 7-E)
Supervisor engines supported	Supervisor 7-E Supervisor 7L-E	Supervisor 7-E Supervisor 7L-E	Supervisor 7-E Supervisor 7L-E	Supervisor 7-E
Maximum PoE per slot	1,500W	1,500W	1,500W	1,500W slots 1 and 2, 750W slots 3,4,7-10
Bandwidth scalability per line-card slot	Up to 48 Gbps on all slots	Up to 48 Gbps on all slots	Up to 48 Gbps on all slots	Up to 48 Gbps on all slots[5]
Number of power supply bays	2	2	2	2
AC input power	Yes	Yes	Yes	Yes
DC Input power	Yes	Yes	Yes	Yes
Integrated Power over Ethernet	Yes	Yes	Yes	Yes

[2] Slot 1 is reserved for supervisor engine only; slots 2 and higher are reserved for line cards.
[3] Slots 3 and 4 are reserved for supervisor engines only in Cisco Catalyst 4507R-E and 4507R+E; slots 1-2 and 5-7 are reserved for line cards
[4] Slots 5 and 6 are reserved for supervisor engines only in Cisco Catalyst 4510R-E and 4510R+E; slots 1-4 and 7-10 are reserved for line cards

Feature	Cisco Catalyst WS-C4503-E Chassis	Cisco Catalyst WS-C4506-E Chassis	Cisco Catalyst WS-C4507R+E Chassis	Cisco Catalyst WS-C4510R+E Chassis
Minimum number of power supplies	1	1	1	1
Power supplies supported	● 1000W AC ● 1400W AC ● 1300W ACV ● 2800W ACV ● 4200W ACV ● 6000W ACV ● 1400W DC (triple input) ● 1400W-DC-P	● 1000W AC ● 1400W AC ● 1300W ACV ● 2800W ACV ● 4200W ACV ● 6000W ACV ● 1400W DC (triple input) ● 1400W-DC-P	● 1000W AC ● 1400W AC ● 1300W ACV ● 2800W ACV ● 4200W ACV ● 6000W ACV ● 1400W DC (triple input) ● 1400W-DC-P	● 1400W AC ● 2800W ACV ● 4200W ACV ● 6000W ACV ● 1400W DC (triple input) ● 1400W-DC-P
Number of fan-tray bays	1	1	1	1
Location of 19-inch rack mount	Front	Front	Front	Front
Location of 23-inch rack mount	Front (option)	Front (option)	Front (option)	Front (option)

Cisco Catalyst 4500 Series line cards can be mixed and matched to suit numerous LAN access, server connectivity, or branch-office deployments. .The Cisco Catalyst 4500 Series supports the following line cards, by product number:

Product Number /Description
Cisco Catalyst 4500E Series Line Cards
WS-X4748-UPOE+E Cisco Catalyst 4500E Series 48-Port UPOE 10/100/1000 (RJ-45) **WS-X4748-RJ45V+E** Cisco Catalyst 4500E Series 48-Port 802.3at PoEP 10/100/1000 (RJ-45) **WS-X4748-RJ45-E** Cisco Catalyst 4500E Series 48-Port 10/100/1000 (RJ-45) **WS-X4712-SFP+E** Cisco Catalyst 4500E Series 12-port 10 Gigabit Ethernet (SFP+) **WS-X4624-SFP-E** Cisco Catalyst 4500E Series 24-port GE (SFP) **WS-X4612-SFP-E** Cisco Catalyst 4500E Series 12-port GE (SFP) **WS-X4648-RJ45V-E** Cisco Catalyst 4500E Series 48-Port PoE 10/100/1000(RJ45) **WS-X4648-RJ45V+E** Cisco Catalyst 4500E Series 48-Port Premium PoE 10/100/1000(RJ45) **WS-X4606-X2-E** Cisco Catalyst 4500E Series 6-Port 10GE (X2) **WS-X4648-RJ45-E** Cisco Catalyst 4500E Series 48-Port Data 10/100/1000(RJ45)

Cisco Catalyst 4500 Classic 10/100 Line Cards
WS-X4148-RJ Cisco Catalyst 4500 10/100 Auto Module, 48-Port (RJ-45) **WS-X4248-RJ45V** Cisco Catalyst 4500 PoE 802.3af 10/100, 48-Port (RJ-45)
Cisco Catalyst 4500 Classic 10/100/1000 Line Cards
WS-X4548-GB-RJ45 Cisco Catalyst 4500 Enhanced 48-Port 10/100/1000 Module (RJ-45) **WS-X4548-RJ45V+** Cisco Catalyst 4500 48-Port 802.3af PoE and 802.3at PoEP 10/100/1000 (RJ-45) **WS-X4548-GB-RJ45V** Cisco Catalyst 4500 PoE IEEE 802.3af 10/100/1000, 48 Ports (RJ-45)
Cisco Catalyst 4500 Classic 100 BASE-X FE Line Cards
WS-X4248-FE-SFP Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-Port 100BASE-X (SFP)
Cisco Catalyst 4500 Classic 1000 BASE-X GE Line Cards
WS-X4306-GB Cisco Catalyst 4500 Gigabit Ethernet Module, 6 Ports (GBIC) **WS-X4506-GB-T** Cisco Catalyst 4500 6-Port 10/100/1000 RJ-45 PoE IEEE 802.3af and 1000BASE-X (SFP) **WS-X4418-GB** Cisco Catalyst 4500 Gigabit Ethernet Module, Server Switching 18 Ports (GBIC) **WS-X4448-GB-SFP** Cisco Catalyst 4500 Gigabit Ethernet Module, 48 Ports 1000X (SFP)

The Cisco Catalyst 4500 Series has flexible interface types and port densities that allow network configurations to be mixed and matched to meet the specific needs of the organizations network.

Cisco Catalyst 4500 Series Switching Modules Number of	Number of Interfaces Supported per Line Card	Cisco Catalyst 4503-E	Cisco Catalyst 4506-E	Cisco Catalyst 4507R+E	Cisco Catalyst 4510R+E
Switched 10/100 Fast Ethernet (RJ-45)	48	96	240	240	384
Switched 10/100 Fast Ethernet (RJ-45) with IEEE 802.3af at Power over Ethernet (PoE/PoEP)	48	96	240	240	384
Switched 100 FX Fast Ethernet (MT-RJ)	48	96	240	240	384
Switched 1000BASE-X	6, 18, or 48	104	244	244	388

Cisco Catalyst 4500 Series Switching Modules Number of	Number of Interfaces Supported per Line Card	Cisco Catalyst 4503-E	Cisco Catalyst 4506-E	Cisco Catalyst 4507R+E	Cisco Catalyst 4510R+E
(Fiber)					
Switched 10/100/1000BASE-T Gigabit Ethernet	48	96	240	240	384
Switched 10/100/1000BASE-T Gigabit Ethernet with IEEE 802.3af at PoE/PoEP	48	96	240	240	384
Switched 10/100/1000BASE-T Gigabit Ethernet with UPOE	48	96	240	240	384
Switched 10 Gigabit Ethernet	6 or 12	24	60	60[6]	96[7]

The Cisco Catalyst 4500-X Series Switch is a fixed 10 Gigabit Ethernet aggregation platform that provides flexibility through two versions of base switches along with optional uplink module. Both the 32- and 16-port versions can be configured with optional network modules and offer similar features. The Small Form-Factor Pluggable Plus (SFP+) interface supports both 10 Gigabit Ethernet and 1 Gigabit Ethernet ports, allowing upgrades to 10 Gigabit Ethernet when organizational demands change. The uplink module is hot swappable.

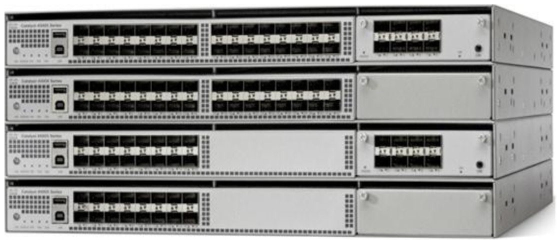
Deployment Options include:

- 16- and 32-port 10 Gigabit Ethernet Small Form-Factor Pluggable Plus (SFP+) models
- 8-port 10 Gigabit Ethernet SFP+ removable uplink module
- Dual-redundant AC/DC power supply and five field-replaceable unit (FRU) fans

The figure below shows the Cisco Catalyst 4500-X Series Switch with and without the optional 8-port uplink module and back of the switch.

---

[6] WS-C4507R-E and WS-C4510R-E chassis support up to 34 switched 10 Gigabit Ethernet ports
[7] WS-C4507R-E and WS-C4510R-E chassis support up to 34 switched 10 Gigabit Ethernet ports




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. TOE access

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 (assigned the appropriate privilege level), all use of the user identification mechanism, any use of the authentication mechanism, any change in the configuration of the TOE, any matching of packets to access control entries in ACLs when traversing the TOE; and any failure of a packet to match an access control list (ACL) rule allowing traversal of the TOE. The TOE will write audit records to the local logging buffer by default and can be configured to send audit data via syslog to a remote audit server, or display to the local console. 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 operated in FIPS mode. The crypto module is FIPS 140-2 SL2 validated (certificate number 1942). 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-SHA1The TOE also implements SSHv2 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 1942).

1.7.3 Traffic Filtering and Switching (VLAN Processing and ACLs)

VLANs control whether Ethernet frames are passed through the switch interfaces based on the VLAN tag information in the frame header. IP ACLs or ICMP ACLs control whether routed IP packets are forwarded or blocked at Layer 3 TOE interfaces (interfaces that have been configured with IP addresses). VACLs (using access mapping) control whether non-routed frames (by inspection of MAC addresses in the frame header) and packets (by inspection of IP addresses in the packet header) are forwarded or blocked at Layer 2 ports assigned to VLANs. The TOE examines each frame and packet to determine whether to forward or drop it, on the basis of criteria specified within the VLANs access lists and access maps applied to the interfaces through which the traffic would enter and leave the TOE. For those interfaces configured with Layer-3 addressing the ACLs can be configured to filter IP traffic using: the source address of the traffic; the destination address of the traffic; and the upper-layer protocol identifier. Layer-2 interfaces can be made part of Private VLANs (PVLANs), to allow traffic to pass in a pre-defined manner among a primary, and secondary (‘isolated’ or ‘community’) VLANs within the same PVLAN.

VACL access mapping is used to match IP ACLs or MAC ACLs to the action to be taken by the TOE as the traffic crosses the interface, causing the packet to be forwarded or dropped. The traffic is matched only against access lists of the same protocol type; IP packets can be matched against IP access lists, and any Ethernet frame can be matched against MAC access lists. Both IP and MAC addresses can be specified within the VLAN access map.

Use of Access Control Lists (ACLs) also allows restriction of remote administration connectivity to specific interfaces of the TOE so that sessions will only be accepted from approved management station addresses identified as specified by the administrator.

The TOE supports routing protocols including BGPv4, EIGRP, EIGRPv6 for IPv6, RIPv2, and OSPFv2 to maintain the routing tables. The routing tables can also be configured and maintained manually. Since routing tables are used to determine which egress ACL is applied, the authority to modify the routing tables is restricted to authenticated administrators and authenticated neighbor routers. The only aspects of the routing protocol that is security relevant in this TOE is the ability to authenticate neighbor routers using shared passwords. Other security features and configuration options of routing protocols are beyond the scope of this Security Target and are described in administrative guidance.

The TOE supports VACLs (VLAN ACLs), which can filter traffic traversing VLANs on the TOE based on IP addressing and MAC addressing.

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 supports use of a remote AAA server (RADIUS and TACACS+) as the enforcement point for identifying and authenticating users, including login and password dialog, challenge and response, and messaging support. For RADIUS, only the password is encrypted, while TACACS+ encrypts the entire packet body except the header. 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.

The TOE also supports authentication of other routers using router authentication supported by BGPv4, EIGRP, EIGRPv6 for IPv6, RIPv2, and OSPFv2. 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.

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 through either a secure session via SSHv2, 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,
- create, modify, or delete information flow policies,

- create, modify, or delete routing tables,
- modify and set session inactivity thresholds,
- modify and set the time and date,
- and create, delete, and review the audit trail

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

The TOE switch platform maintains administrative privilege level and non-administrative access. Non-administrative access is granted to authenticated neighbor routers for the ability to receive updated routing tables per the information flow rules. There is no other access or functions associated with non-administrative access. The administrative privilege levels include:

- Administrators are assigned to privilege levels 0 and 1. Privilege levels 0 and 1 are defined by default and are customizable. These levels have a very limited scope and access to CLI commands that include basic functions such as login, show running system information, turn on/off privileged commands, logout.
- Semi-privileged administrators equate to any privilege level that has a subset of the privileges assigned to level 15; levels 2-14. These levels are undefined by default and are customizable. The custom level privileges are explained in the example below.
- Privileged administrators are equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15.

The term “authorized administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; 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 separate parts of the TOE (encrypted sessions for remote administration (via SSHv2)). A separate VLAN should be used to ensure the routing protocol communications between the TOE and neighbor routers (including routing table updates and neighbor router authentication) is logically isolated from the traffic on other VLANs..

The TOE also supports replay detection, though it is only applicable to the encrypted sessions for remote administration via SSHv2. 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 TOE Access

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

The TOE can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

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 and HTTPS Server for web user interface management sends authentication data in the clear and does not enforce the required privilege levels. This feature is enabled by default. The HTTP and the HTTPS Server needs to be disabled and should not be configured for use. Not including this feature does not interfere with the management of TOE as defined in the Security Target.
- IEEE 802.11 Wireless Standards the evaluated configuration of Catalyst Switches as described is this Security Target does not support implementing wireless local area network, as it requires additional hardware beyond what is included in the evaluated configuration.
- MAC address filtering restricts a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. The SFPs in the Security Target are defined as information flow polices, not access polices that allow access based on MAC address. This feature is disabled by default and cannot be configured for use, as it may interfere with the enforcement of the security policies as defined in the Security Target.
- 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.
- 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.
- VPN enabling and configuring VPN requires additional licenses beyond what is included in the evaluated configuration.
- Flexible NetFlow - is used for a traffic optimization, and SFRs do not include performance/optimization features. 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.

- TrustSec - is only relevant to this ST to a limited degree, for RADIUS KeyWrap, which is being represented with other cryptographic methods. This feature is disabled by default and can be configured for use. Not including this feature does not interfere with the enforcement of the security policies as defined in the Security Target.
- VLAN Trunking, 802.1Q tunneling, VLAN mapping, dynamic VLAN membership. These features are disabled by default and should remain disabled in the evaluated configuration. Not including these features do not interfere with the enforcement of the security policies as defined in the Security Target.
- The Network Assistant application and CiscoWorks LAN Management Solutions are separate licensed, separate products and are not included in the scope of this evaluation.
- Security Group Tags are a 16-bit single label indicating the security classification of a source in the TrustSec domain and it is appended to an Ethernet frame or an IP packet. This feature is disabled by default and can be configured for use. 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.

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 (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) comprises:

- Installation and Configuration for Common Criteria EAL2 Evaluated Cisco IOS Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X)
- Administrative Guidance for Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X)
- 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

This ST and the TOE it describes are conformant to the following package:

- EAL2 Augmented (ALC_DVS.1 and ALC_FLR.2)

2.2 Protection Profile Conformance Claim

This ST and TOE it describes is not claiming conformance to any Protection Profile.

3 SECURITY PROBLEM DEFINITION

This section describes the security environment in which the TOE is intended to be used.

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 4 TOE Assumptions

Assumption	Assumption Definition
A.NOEVIL	All authorized administrators are assumed not evil and will not disrupt the operation of the TOE intentionally.
A.TRAIN_AUDIT	Administrators will be trained to periodically review audit logs to identify sources of concern
A.TRAIN_GUIDAN	Personnel will be trained in the appropriate use of the TOE to ensure security.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.CONFIDENTIALITY	Copies of TOE configuration data including representations of authentication data maintained off the TOE in hard-copy or soft-copy will be kept confidential and access will be limited to authorized administrators. Audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic.
A.INTEROPERABILITY	The TOE will be able to function with the software and hardware of other switch vendors on the network.
A.LOWEXP	The threat of malicious attacks aimed at exploiting the TOE is considered low.

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 5 Threats

Threat	Threat Definition
T.AUDIT_REVIEW	Actions performed by users may not be known to the administrators due to actions not being recorded locally or remotely in a manner suitable for allow interpretation of the messages.
T.AUTHADMIN	An authorized administrative user may either intentionally or unintentionally gain access to the configuration services for which the user is not authorized.
T.MEDIATE	An unauthorized entity may send impermissible information through the TOE which results in the exploitation of network, the recipient of the network traffic.

Threat	Threat Definition
T.NOAUDIT	An unauthorized user modifies or destroys audit data.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE to disrupt operations of the TOE.
T.NOMGT	The administrator is not able to manage the security functions of the TOE, resulting in the potential for the TOE configuration to compromise security objectives and policies.
T.UNAUTH_MGT_ACCESS	An unauthorized user gains management access to the TOE and views or changes the TOE security configuration.
T.TIME	Evidence of a compromise or malfunction of the TOE may go unnoticed or not be properly traceable if recorded events are not properly sequenced through application of correct timestamps.
T.USER_DATA_REUSE	User data that is temporarily retained by the TOE in the course of processing network traffic could be inadvertently re-used in sending network traffic to a destination other than intended by the sender of the original network traffic.

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 6 Organizational Security Policies

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4 SECURITY OBJECTIVES

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

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

4.1 Security Objectives for the TOE

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

Table 7 Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
O.ACCESS_CONTROL	The TOE will restrict access to the TOE Management functions to the authorized administrators.
O.ADMIN_ROLE	The TOE will provide administrator levels to isolate administrative actions, and to make the administrative functions available locally and remotely.
O.AUDIT_GEN	The TOE will generate audit records which will include the time that the event occurred and if applicable, the identity of the user performing the event.
O.AUDIT_VIEW	The TOE will provide only the authorized administrators the capability to review and to configure the TOE to transmit audit messages to a remote syslog server.
O.CFG_MANAGE	The TOE will provide management tools/applications to allow authorized administrators to manage its security functions.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access.
O.MEDIATE	The TOE must mediate the flow of all information between hosts located on disparate internal and external networks governed by the TOE.
O.SELFPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.STARTUP_TEST	The TOE will perform initial startup tests upon bootup of the system to ensure correct operation of the cryptographic module, TOE software image, and TOE configuration.
O.TIME	The TOE will provide a reliable time stamp for its own use.

TOE Objective	TOE Security Objective Definition
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.

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 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 8 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.AUDIT_REVIEW	Administrators will be trained to periodically review the audit logs to identify sources of concern and will make a syslog server available for use by the TOE and TOE administrators.
OE.CONFIDENTIALITY	The hard copy documents and soft copy representations that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to Authorized administrators. Audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic.
OE.INTEROPERABILITY	The TOE will be able to function with the software and hardware of other vendors on the network.
OE.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
OE.LOWEXP	The threat of malicious attacks aimed at exploiting the TOE is considered low.
OE.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error.
OE.TRAIN_GUIDAN	Personnel will be trained in the appropriate use of the TOE to ensure security and will refer to all administrative guidance to ensure the correct operation of the TOE.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, dated: July 2009* and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: 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 …").
- Extended Requirements (i.e., those not found in Part 2 of the CC) are identified with "_EXT" in of the functional class/name.
- 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. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 9 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_SAR.1: Audit review
	FAU_STG.1: Protected audit trail storage
FCS: Cryptographic support	FCS_CKM.1(1): Cryptographic key generation - RSA
	FCS_CKM.1(2): Cryptographic key generation - AES
	FCS_CKM.4: Cryptographic key zeroization
	FCS_COP.1(1): Cryptographic operation (for RSA encryption/decryption)
	FCS_COP.1(2): Cryptographic operation (for AES encryption/decryption)
	FCS_COP.1(3): Cryptographic operation (for RNG)

Functional Component	
	FCS_COP.1(4) Cryptographic operation (for MD5 hashing)
	FCS_COP.1(5) Cryptographic operation (for cryptographic hashing)
	FCS_COP.1(6) Cryptographic operation (for keyed-hash message authentication)
	FCS_SSH_EXT.1: SSH
FDP: User data protection	FDP_ACC.2: Complete access control (PRIVAC)
	FDP_ACF.1: Security attribute based access control (PRIVAC)
	FDP_IFC.1(1) Subset Information Flow Control – VLAN
	FDP_IFC.1(2) Subset Information Flow Control - ACL
	FDP_IFC.1(3) Subset Information Flow Control - VACL
	FDP_IFF.1(1) Simple Security Attributes – VLAN
	FDP_IFF.1(2) Simple Security Attributes – ACL
	FDP_IFF.1(3) Simple Security Attributes – VACL
	FDP_RIP.2: Full residual information protection
FIA: Identification and authentication	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UAU.5: Password-based authentication mechanism
	FIA_UAU.7: Protected authentication feedback
	FIA_UID.2 User identification before any action
FMT: Security management	FMT_MOF.1 Management of Security Functions Behavior
	FMT_MSA.2 Secure Security Attributes
	FMT_MSA.3(1) Static Attribute Initialization (Traffic Flow)
	FMT_MSA.3(2) Static Attribute Initialization (Access Control)
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_RPL.1: Replay detection
	FPT_STM.1: Reliable time stamps
	FPT_TST_EXT.1: TSF testing
FTA: TOE Access	FTA_SSL.3: TSF-initiated termination
	FTA_TAB.1: Default TOE Access Banners

5.2.1 Security audit (FAU)

5.2.1.1 FAU_GEN.1: Audit data generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [***not specified***] level of audit **specified in Table 10**; and

c) [**no additional events**].

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(if applicable), 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 the Additional Audit Record Contents column of Table 10**].

Table 10: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_SAR.1	None.	
FAU_STG.1	None.	
FCS_SSH_EXT.1	Failure to establish an SSH session Establishment/Termination of an SSH session	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_ACC.2	None	None
FDP_ACF.1	All decisions on request for access control (execute a command)	None
FDP_IFC.1(1),(2),(3)	None	
FDP_IFF.1(1)	None	
FDP_IFF.1(2)	All decisions on requests for information flow	None.
FDP_IFF.1(3)	IP packet flows denied by VACL	None

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UAU.2	All use of the authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.5	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UID.2	All use of the identification mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	None
FMT_MSA.3(1)(2)	Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security attributes.	None
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TST_EXT.1	Indication that TSF self-test was completed.	Any additional information generated by the tests beyond “failure”.

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_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [**privileged administrator, and semi-privileged administrator with appropriate privileges**] with the capability to read [**all TOE audit trail data**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.1.4 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent***] ~~unauthorised~~ modifications to the stored audit records in the audit trail.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1(1): Cryptographic key generation - RSA

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA**] and specified cryptographic key sizes [**1024 bits and 2048 bits**] that meet the following: [**FIPS 186-3**].

5.2.2.2 FCS_CKM.1(2) Cryptographic key generation – AES

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**none**] and specified cryptographic key sizes [**128-bits, 256-bits**] that meet the following: [**RNG as specified in FCS_COP.1(3)**].

5.2.2.3 FCS_CKM.4: Cryptographic key zeroization

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

5.2.2.4 FCS_COP.1(1) Cryptographic operation (for RSA encryption/decryption)

FCS_COP.1.1(1) The TSF shall perform [**encryption and decryption of keying material**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**1024-bits and 2048-bits**] that meet the following: [**none**].

5.2.2.5 FCS_COP.1(2): Cryptographic operation (for AES encryption/decryption)

FCS_COP.1.1(2) 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**] that meet the following:

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

5.2.2.6 FCS_COP.1(3): Cryptographic operation (for RNG)

FCS_COP.1.1(3) The TSF shall perform [**Random Number Generation**] in accordance with a specified cryptographic algorithm [**RNG using AES]** and cryptographic key sizes [**256 bits**] that meet the following: [**SP 800-90 DRBG as specified in FIPS 140-2 Annex C**].

5.2.2.7 FCS_COP.1(4) Cryptographic operation (for MD5 hashing)

FCS_COP.1.1(4) The TSF shall perform [**secure hash (message digest)**] in accordance with a specified cryptographic algorithm: [**MD5**] and cryptographic key sizes [**128-bit hash value**] that meet the following: [**MD5 RFC 1321 as applied in OSPFv2 (RFC 2328), RIPv2 (RFC 2453), BGPv4 (RFC 2385), and EIGRP, and EIGRPv6 (Cisco proprietary)**].

5.2.2.1 FCS_COP.1(5) Cryptographic operation (for cryptographic hashing)

FCS_COP.1.1(5) The TSF shall perform [**cryptographic hashing services**] in accordance with a specified cryptographic algorithm [**SHA-1] and message digest sizes** [**160**] **bits** that meet the following: [**FIPS Pub 180-3 "Secure Hash Standard"**].

5.2.2.2 FCS_COP.1(6): Cryptographic operation (for keyed-hash message authentication)

FCS_COP.1.1(6) The TSF shall perform [**keyed-hash message authentication**] in accordance with a specified cryptographic algorithm [**HMAC-SHA-1**], and cryptographic ~~key~~ **message digest** size [**160 bits**] that meet the following: [**FIPS Pub 198-1 "The Keyed-Hash Message Authentication Code", and FIPS PUB 180-3, "Secure Hash Standard."**].

5.2.2.3 FCS_SSH_EXT.1: SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed upon request from the SSH client.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of 120 seconds, and provide a limit to the number of failed authentication attempts a client may perform in a single session to 3 attempts.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: password-based.

FCS_SSH_EXT.1.5 The TSF shall ensure that, as described in RFC 4253, packets greater than 35,000 bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms AES-CBC-128 and AES-CBC-256.

FCS_SSH_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [no other public key algorithms,] as its public key algorithm(s).

FCS_SSH_EXT.1.8 The TSF shall ensure that data integrity algorithms used in the SSH transport connection is hmac-sha1, hmac-sha1-96, hmac-md5.

FCS_SSH_EXT.1.9 The TSF shall ensure that diffie-hellman-group14-sha1 is an allowed key exchange method used for the SSH protocol.

5.2.3 User data protection (FDP)

5.2.3.1 FDP_ACC.2 Complete access control (PRIVAC)

FDP_ACC.2.1 The TSF shall enforce the [**Privileged Based Access Control SFP**] on [**Subjects: Authenticated Administrators; Objects: CLI Commands**] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

5.2.3.2 FDP_ACF.1 Security attribute based access control (PRIVAC)

FDP_ACF.1.1 The TSF shall enforce the [**Privileged Based Access Control SFP**] to objects based on the following: [

Subject security attributes:

- **Authenticated Administrators:**
  - **User Identity (identity of the administrator)**
  - **Privilege Levels – (the set of privilege levels assigned to the Authenticated Administrator.**

Object security attributes:

- **CLI Commands**

- **Privilege Level– The privilege level that an Authenticated Administrator must be assigned in order to execute commands**
- **Password (if password has been set for a command or command set)**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- **Authenticated Administrators whose privilege level includes the command, and has the password if applicable**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**Authenticated Administrators whose privilege level is set to level 15**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**none**].

5.2.3.3 FDP_IFC.1(1) Subset Information Flow Control – VLAN

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

a) Controlled subjects: Layer 2 ports (i.e. ports configured as switch ports);

b) Controlled information: Ethernet Frames;

c) Operation: permit or deny OSI Layer 2 (Data Link Layer) communication].

5.2.3.4 FDP_IFF.1(1) Simple Security Attributes – VLAN

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

a) security attributes of controlled subjects:

- **Receiving/transmitting Layer 2 port identifier (e.g. slot/port);**
- **VLAN assigned to the port**
- **PVLAN assigned to the port**

b) security attributes of controlled information:

- **VLAN tag in an Ethernet Frame Header**].

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

- **the source and destination Layer 2 ports are configured to be in the same VLAN or**

- **the frames have been permitted into the VLAN through traffic flow controls enforced at Layer 3 as defined in FDP_IFF.1(2)**].

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

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules: [

When the ingress port is part of a PVLAN:

- **Traffic entering a promiscuous port can be forwarded through all ports within the same PVLAN, including the isolated and community ports.**
- **Traffic entering an isolated port can be forwarded only through promiscuous ports.**
- **Traffic entering a community port can be forwarded only through other ports in the same community and through promiscuous ports**].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [

When the ingress port is not part of a PVLAN:

- **The VLAN tag in the frame packets does not match the VLAN of the ingress port associated with a VLAN will not be forwarded to VLAN interfaces (subjects) not configured to be in that VLAN**

When the ingress port is part of a PVLAN:

- **Traffic entering an isolated port has complete Layer 2 separation from the other isolated and community ports within the same PVLAN, and from ports outside the PVLAN**
- **Traffic entering a community port has complete Layer 2 separation from all other interfaces in other communities and from isolated ports within the same PVLAN, and from ports outside the PVLAN**].

5.2.3.5 FDP_IFC.1(2) Subset Information Flow Control - ACL

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

a) Controlled subjects: Layer 3 interfaces (i.e. any interface configured with an IP address including physical copper

or fiber ports, or any virtual sub-interface, or Layer 3 VLAN interface);

b) **Controlled information: IP packets**

c) **Operation: forward or drop the packets**].

5.2.3.6 FDP_IFF.1(2) Simple Security Attributes - ACL

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

a) **security attributes of controlled subjects:**
   - **Interface ID (e.g. physical slot/port identifier, or logical port-channel identifier, or VLAN interface identifier);**
   - **IP address assigned to the interface**

b) **security attributes of controlled information:**
   - **source IP address identified within the packet;**
   - **destination IP address identified within the packet;**
   - **transport layer protocol number (e.g. UDP, TCP);**
   - **network layer protocol number (e.g. IPv4, IPv6, ICMPv4, ICMPv6, ESP, AH, etc.);**
   - **ICMP type**].

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

- **all the information security attribute values are unambiguously permitted by the information flow security policy rules (IP ACLs or ICMP), where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;**
- **the source IP address in the information (packet), correlates to network address in the routing table, which in turn correlates to the TOE interface that received the packet;**
- **and the destination IP address in the information (packet), correlates to connected network in the routing table**].

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

FDP_IFF.1.4(2) The TSF shall explicitly authorize an information flow based on the following rules: [**none**].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: [

a) **The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed IP address of the source subject is an external IT entity on an internal network;**

b) **The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed IP address of the source subject is an external IT entity on the external network;**

c) **The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed IP address of the source subject is an external IT entity on a broadcast network;**

d) **The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed IP address of the source subject is an external IT entity on the loopback network.**

e) **The TOE shall drop requests in which the information received by the TOE does not correspond to an entry in the routing table**].

5.2.3.7 FDP_IFC.1(3) Subset Information Flow Control – VACL

FDP_IFC.1.1(3) The TSF shall enforce the [**VACL SFP**] on: [

a) **Controlled subjects: VLANs configured on the TOE;**

b) **Controlled information: Ethernet frames (with or without IP packet headers)**

c) **Operation: forward, drop, forward capture, or redirect the frames**].

5.2.3.8 FDP_IFF.1(3) Simple Security Attributes - VACL

FDP_IFF.1.1(3) The TSF shall enforce the [**VACL SFP**] based on the following types of subject and information security attributes: [

a) **security subject attributes:**
   - **VLAN ID**
   - **VLAN access-map containing one or more map sequences each with a match clause and an action clause**

b) **security information attributes:**
   - **Ethernet frame header attributes (when MAC ACLs are specified in a match clause)**

        - **source MAC address identified within the packet;**
        - **destination MAC address identified in the packet;**
        - **EtherType (e.g. 0x0800 for IPv4)**
    - **IP packet header attributes (when IP ACLs are specified in a match clause):**
        - **source IP address identified within the packet;**
        - **destination IP address identified within the packet;**
        - **transport layer protocol number (e.g. UDP, TCP)**].

FDP_IFF.1.2(3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- **all the information security attribute values are unambiguously permitted by the information flow security policy rules (VACLs), where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator**].

FDP_IFF.1.3(3) The TSF shall enforce the [**if an empty or undefined ACL is specified in the match clause of the access-map, any packet/frame will match the match clause, and the action defined in the associated action clause will be taken for all packets/frames**].

FDP_IFF.1.4(3) The TSF shall explicitly authorize an information flow based on the following rules: [**IGMP packets are not checked against VACLs (but can be checked via ACLs defined in FDP_IFF.1(2))**].

FDP_IFF.1.5(3) The TSF shall explicitly deny an information flow based on the following rules: [**the source MAC address is explicitly denied in a specified VLAN through use of the 'mac-address-table static' command with the keyword 'drop'**].

5.2.3.9 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_ATD.1: User attribute definition

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

- **Interactive (human) users:**
  - **user identity;**
  - **privilege levels; and**
  - **password**
- **Neighbor Routers**
  - **IP address and**
  - **password**].

5.2.4.2 FIA_UAU.2: User identification before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.4.3 FIA_UAU.5: Password-based authentication mechanism

FIA_UAU.5.1 The TSF shall provide [**local password-based authentication, remote password-based authentication via RADIUS and TACACS+, and neighbor router authentication**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**administratively-defined sequence in which authentication mechanisms should be used**].

5.2.4.4 FIA_UAU.7: Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide ~~only~~ [**no feedback, nor any locally visible representation of the user-entered password**] to the user while the authentication is in progress.

5.2.4.5 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.5 Security management (FMT)

5.2.5.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [***determine the behavior of***] the functions [

- **Audit trail (create, delete, review)**
- **Network traffic (information flow) rules (create, delete, modify, and view)**
- **Routing tables (create, modify, delete)**
- **Session inactivity (set, modify threshold limits)**
- **Time determination (set, change date/timestamp)**
- **TSF self test (TOE and cryptographic module)**] to [**privileged administrator, and semi-privileged administrator with appropriate privileges**].

5.2.5.2 FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [**security attributes that are considered in the VLAN SFP, VACL SFP, ACL SFP, and PRIVACL SFP**].

5.2.5.3 FMT_MSA.3(1) Static Attribute Initialization (Traffic Flow)

FMT_MSA.3.1(1) The TSF shall enforce the [**VLAN SFP, VACL SFP, and ACL SFP**], to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [**privileged administrator, and semi-privileged administrator with appropriate privileges**] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.4 FMT_MSA.3(2) Static Attribute Initialization (Access Control)

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

FMT_MSA.3.2(2) The TSF shall allow the [**privileged administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.5 FMT_MTD.1: Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [***modify***] the [**all TOE data**] to [**privileged administrator, and semi-privileged administrator with appropriate privileges**].

5.2.5.6 FMT_SMF.1: Specification of Management Functions

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

- **Ability to manage the cryptographic functionality**
- **Ability to manage routing tables**
- **Ability to manage the audit logs and functions**
- **Ability to manage information flow control attributes**
- **Ability to manage security attributes belonging to individual users**
- **Ability to manage the default values of the security attributes**
- **Ability to manage the warning banner message and content**
- **Ability to manage the time limits of session inactivity**].

5.2.5.7 FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the **following** ~~roles~~ **administrative privilege levels and non-administrative access [0, 1(administrator), 15 (privileged administrator), custom levels 2-14 (semi-privileged administrator), non-administrative access (neighbor routers)**].

FMT_SMR.1.2 The TSF shall be able to associate users with ~~roles~~ **administrative privilege levels and non-administrative access**.

Application note: The term "authorized administrator" is used in this ST to refer to any user which has been granted rights equivalent to a privileged administrator or semi-privileged administrator.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 FPT_RPL.1: Replay detection

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

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

5.2.6.2 FPT_STM.1: Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.6.3 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 TOE Access (FTA)

5.2.7.1 FTA_SSL.3: TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate **a remote and local** interactive session after a [**authorized administrator-configurable time interval of session inactivit**y].

5.2.7.2 FTA_TAB.1: Default TOE Access Banners

FTA_TAB.1.1 Before establishing a ~~user~~ **local or remote administrator** session the TSF shall display an **authorized administrator-specified** advisory **notice and consent** warning message regarding unauthorized use of the TOE.

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 (Table 11).

Extended Requirements Rationale:

FCS_SSH_EXT.1:

This SFR was modeled from the NDPP – where it is defined as a requirement specific to SSHv2 protocol supported by the TOE.

Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's implementation of the protocol.

FPT_TST_EXT.1:

This SFR was modeled from the NDPP – where it is defined as a requirement for TSF self tests of the TOE during initialization (on bootup). Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's implementation of the testing functionality.

5.4 TOE SFR Dependencies Rationale

The following table provides dependency rational for SFRs defined in this ST.

Table 11: SFR Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Met by FAU_GEN. Met by FIA_UID.2
FAU_SAR.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_STG.1	FAU_GEN.1	Met by FAU_GEN.1
FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Met by FCS_COP.1(1) Met by FCS_CKM.4
FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Met by FCS_COP.1(2) Met by FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Met by FCS_CKM.1
FCS_COP.1(1)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Met by FCS_CKM.1(1) and FCS_CKM.4
FCS_COP.1(2)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Met by FCS_CKM.1(2) and FCS_CKM.4
FCS_COP.1(3)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	See rationale below for FCS_COP.1(3) and FCS_CKM.4
FCS_COP.1(4)	FDP_ITC.1 or 2 or FCS_CKM.1	See rationale below for FCS_COP.1(4) and

SFR	Dependency	Rationale
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1(5)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	See rationale below for FCS_COP.1(5) FCS_CKM.4
FCS_COP.1(6)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	See rationale below for FCS_COP.1(6) FCS_CKM.4
FCS_SSH_EXT.1	FCS_COP.1	Met by FCS_COP.1
FDP_ACC.2	FDP_ACF.1	Met by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Met by FDP_ACC.2 and FMT_MSA.3(2)
FDP_IFC.1(1)	FDP_IFF.1	Met by FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1	Met by FDP_IFF.1(2)
FDP_IFC.1(3)	FDP_IFF.1	Met by FDP_IFF.1(3)
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(1) and FMT_MSA.3(1)
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(2) and FMT_MSA.3(1)
FDP_IFF.1(3)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFF.1(3) and FMT_MSA.3(1)
FDP_RIP.2	No dependencies	N/A
FIA_ATD.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1	Met by FIA_UID.2
FIA_UAU.5	No dependencies	N/A
FIA_UAU.7	FIA_UAU.1	Met by FIA_UAU.2
FIA_UID.2	No dependencies	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Met by SMT_SMF.1 and FMT_SMR.1
FMT_MSA.2	FDP_ACC.1 FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	Met by FDP_ACC.2 FDP_IFC.1(1), (2), (3) FMT_SMR.1 See rational below regarding FMT_MSA.1
FMT_MSA.3(1)(2)	FMT_MSA.1 FMT_SMR.1	Met by FMT_SMR.1 See rational below regarding FMT_MSA.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_UID.2

SFR	Dependency	Rationale
FPT_RPL.1	No dependencies	N/A
FPT_STM.1	No dependencies	N/A
FPT_TST_EXT.1	No dependencies	N/A
FTA_SSL.3	No dependencies	N/A
FTA_TAB.1	No dependencies	N/A

Functional component FMT_MSA.3(1)(2) depends on functional component FMT_MSA.1 Management of security attributes. In an effort to place all the management requirements in a central place, FMT_MOF.1 was used. Therefore, FMT_MOF.1 more than adequately satisfies the concerns of leaving FMT_MSA.1 out of this Security Target.

Functional components FCS_COP.1(3) (RNG), FCS_COP.1(4) (MD5), FCS_COP.1(5) (SHA-1), and FCS_COP.1(6) (HMAC-SHA-1) do not require the dependency on FCS_CKM.1 because their cryptographic operations do not require key generation.

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

The TOE assurance requirements for this ST are EAL2 Augmented with ALC_DVS.1 and ALC_FLR.2 derived from Common Criteria Version 3.1, Revision 3. The assurance requirements are summarized in the table below.

Table 12: Assurance Measures

Assurance Class	Components	Components Description
DEVELOPMENT	ADV_ARC.1	Security Architectural Description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
GUIDANCE DOCUMENTS	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
LIFE CYCLE SUPPORT	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw Reporting Procedures
TESTS	ATE_COV.1	Evidence coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
VULNERABILITY ASSESSMENT	AVA_VAN.2	Vulnerability analysis

5.5.2 Security Assurance Requirements Rationale

This Security Target claims conformance to EAL2 Augmented with ALC_DVS.1 and ALC_FLR.2. 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 that imposes no restrictions on assumed activity on applicable networks. Augmentation was chosen to demonstrate the security measures followed at the developments sites and to address having flaw remediation procedures and correcting security flaws as they are reported and to ensure that TOE users are aware of the corrections and the fixes.

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 13: Assurance Measures

Component	How requirement will be met
ADV_ARC.1	The architecture description provides the justification how the security functional requirements are enforced, how the security features (functions) cannot be bypassed, and how the TOE protects itself from tampering by untrusted active entities. The architecture description also identifies the system initialization components and the processing that occurs when the TOE is brought into a secure state (e.g. transition form a down state to the initial secure state (operational)).
ADV_FSP.2	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.
ADV_TDS.1	The TOE design describes the TOE security functional (TSF) boundary and how the TSF implements the security functional requirements. The design description includes the decomposition of the TOE into subsystems and/or modules, thus providing the purpose of the subsystem/module, the behavior of the subsystem/module and the actions the subsystem/module performs. The description also identifies the subsystem/module as SFR (security function requirement) enforcing, SFR supporting, or SFR non-interfering; thus identifying the interfaces as described in the functional specification. In addition, the TOE design describes the interactions among or between the subsystems/modules; thus providing a description of what the TOE is doing and how.
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.2	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.2	

Component	How requirement will be met
ALC_DEL.1	The Delivery document describes the delivery procedures for the TOE to include the procedure on how to download certain components of the TOE from the Cisco website and how certain components of the TOE are physically delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components.
ALC_DVS.1 ALC_FLR.2	The Lifecycle document(s) describes the security measures and controls that are in place at the development site(s), the security measures and controls that are in place regarding employees, and the security measures and controls that are in place during the development and maintenance of the TOE. These procedures also include the flaw remediation and reporting procedures so that security flaw reports from TOE users can be appropriately acted upon, and TOE users can understand how to submit security flaw reports to the developer.
ATE_COV.1 ATE_FUN.1	The Test document(s) consist of a test plan describes the test configuration, the approach to testing, and how the TSFI (TOE security function interfaces) has been tested against its functional specification as described in the TOE design and the security architecture description. The test document(s) also include the test cases/procedures that show the test steps and expected results, specify the actions and parameters that were applied to the interfaces, as well as how the expected results should be verified and what they are. Actual results are also included in the set of Test documents.
ATE_IND.2	Cisco will provide the TOE for testing.
AVA_VAN.2	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 14: 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 events related to the enforcement of information flow policies, 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 TOE generates an audit record to indicate the TOE is up and operational or is shutting down and all processes are stopping. To ensure audit records are generated for the required auditable events, the TOE must be configured in its evaluated configuration as specified in the AGD documents. This is to ensure that auditing is enabled so that the audit records are being generated for the required auditable events. If the command ‘no logging on’ is entered the TOE is deemed no longer in the evaluated configuration.. 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 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 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). It is noted that this buffer is circular, so newer entries overwrite older entries so that the siz and number of configured entries are not exceeded.Refer to the Guidance documentation 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

TOE SFRs	How the SFR is Met
	which are described in the Guidance documents and IOS CLI. The logs can be saved to flash memory so records are not lost in case of failures or restarts. Refer to the Guidance documentation for configuration syntax and information. The administrator can set the level of the audit records to be displayed on the console or those that are 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 these types of messages are informational; 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 document for complete guidance and command syntax. Note that audit records are transmitted in the clear to the syslog server, though it is stated the syslog server attached to the internal (trusted) network. For audit records of IP packets denied by VACLs (FDP_IFF.1(3)), the first packet of a denied traffic flow is logged. Subsequent messages for the same denied traffic flow are summary messages containing a count of denied packets of that same traffic flow. Though summary messages contain a timestamp for when the summary message was generated, summary messages do not include a timestamp for when each counted packet was denied. Summary messages are generated at 5 minutes intervals or sooner if a packet count "threshold" is reached (defined using the "vlan access-log threshold <packet-count>" command). A separate "log table" is used to count packets for active traffic flows. This log table will count up to 2048 packets. The log table size can be set with the "vlan access-log maxflow <number>" command, and setting the size to 0 will clear the table. Packets are removed from the log table when their summary message is written to syslog. If the log table is full, packets for new flows will not be counted. For VACL logging, a flow is defined as packets with the same IP addresses and Layer 4 (UDP or TCP) port numbers. Following is a sample of the ACL and the logging In this example, standard named access list stan1 denies traffic from 10.1.1.0 0.0.0.255, allows traffic from all other sources, and includes the log keyword. Switch(config)# ip access-list standard stan1 Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log Switch(config-std-nacl)# permit any log Switch(config-std-nacl)# exit Switch(config)# interface gigabitethernet0/1 Switch(config-if)# ip access-group stan1 in Switch(config-if)# end Switch# show logging Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console logging: level debugging, 37 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 37 messages logged

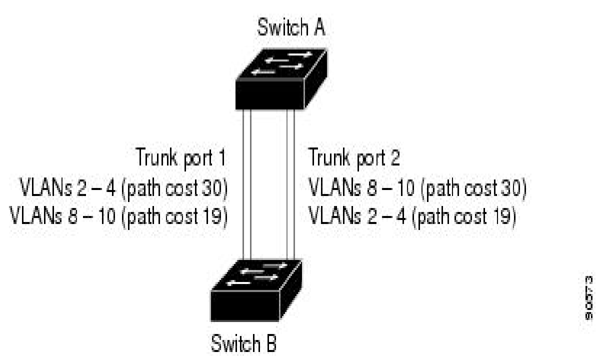
TOE SFRs	How the SFR is Met
	File logging: disabled Trap logging: level debugging, 39 message lines logged Log Buffer (4096 bytes): 00:00:48: NTP: authentication delay calculation problems <output truncated> 00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet 00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet 00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet 00:15:33:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 2009 packets This example is a named extended access list ext1 that permits ICMP packets from any source to 10.1.1.0 0.0.0.255 and denies all UDP packets. Switch(config)# ip access-list extended ext1 Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log Switch(config-ext-nacl)# deny udp any any log Switch(config-std-nacl)# exit Switch(config)# interface gigabitethernet0/3 Switch(config-if)# ip access-group ext1 in This is a an example of a log for an extended IP ACL: 01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1 packet 01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7 packets 01:26:12:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1 packet 01:31:33:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8 packets Note that all logging entries for IP ACLs start with %SEC-6-IPACCESSLOG with minor variations in format depending on the kind of ACL and the access entry that has been matched. This is an example of an output message when the log-input keyword is entered: 00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400) -> 10.1.1.61 (0/0), 1 packet A log message for the same sort of packet using the log keyword does not include the input interface information: 00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0), 1 packet The FIPS crypto tests, the messages are displayed 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

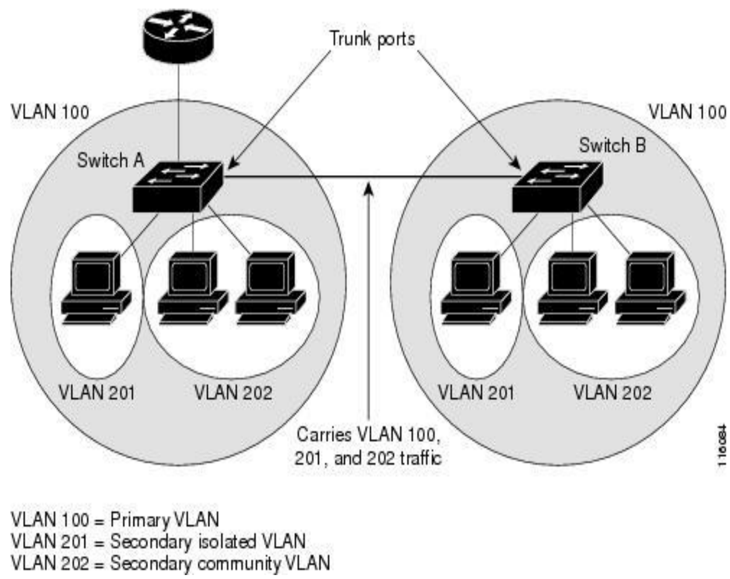
TOE SFRs	How the SFR is Met
	reaching the log-on prompt. If there are issues, the applicable audit record is generated and displayed on the console.

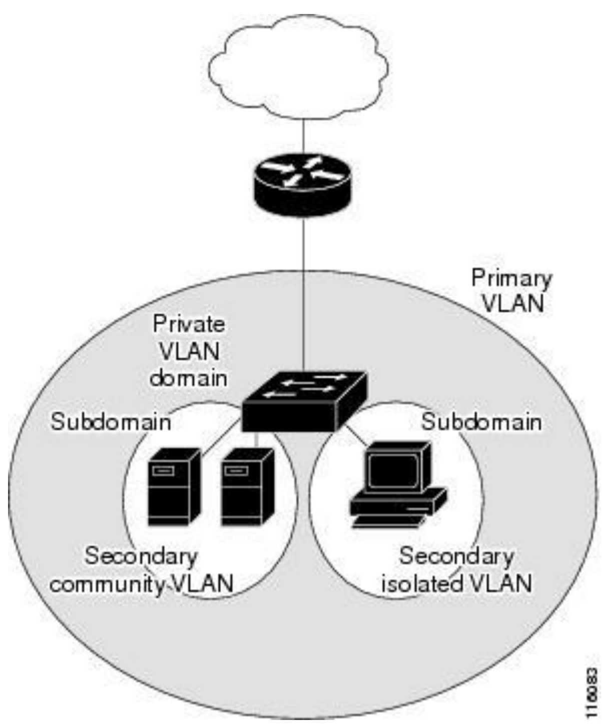
Auditable Event	Rationale
All decisions on requests for information flow through ACLs, and requested denied by VACLs.	The decisions as a result of attempting to send traffic (data) are logged, along with the origin or source of the attempt.
All use of the user identification mechanism.	Events will be generated for attempted identification/ authentication, and the username attempting to authenticate will be included in the log record.
Any use of the authentication mechanism.	Events will be generated for attempted identification/ authentication, and the username attempting to authenticate will be included in the log record, along with the origin or source of the attempt.
Management functions	The use of the security management functions is logged; modifications of the behavior of the functions in the TSF and modifications of default settings.
Changes to the time.	Changes to the time are logged.
Failure to establish and/or establishment/failure of an SSH session	Attempts to establish an SSH session or the failure of an established SSH is logged.
Indication that TSF self-test was completed.	During bootup, if the self-test fails, the failure is logged.

TOE SFRs	How the SFR is Met
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 for configuration syntax and information.
FAU_SAR.1	The TOE provides the interface for the authorized administrator to read all of the TOE audit records. The records include the information described in FAU_GEN.1 above. Refer to the Guidance documentation for commands, configuration syntax and information related to viewing of the audit log files.
FAU_STG.1	The TOE provides the ability for privileged administrators to delete audit records stored within the TOE. The TOE provides dedicated CLI commands that are only available to the privileged administrator to facilitate the deletion of audit records. The local events cannot be altered by any users or mechanisms.

TOE SFRs	How the SFR is Met
	Refer to the Guidance documentation for commands, configuration syntax and information related to viewing of the audit log files.
FCS_CKM.1(1) FCS_COP.1(1)	The TOE generates RSA key establishment schemes conformant with FIPS 186-3. RSA keys are used for encryption and decryption of keying material in SSHv2 used for remote administration of the TOE. (Refer to FIPS 140-2 certificate # 1942)
FCS_CKM.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys through the module securely administering both cryptographic keys and other critical security parameters (CSPs) such as passwords. (Refer to FIPS 140-2 certificate #s 1942)
FCS_CKM.1(2) FCS_COP.1(2) FCS_COP.1(3)	AES is used for RADIUS KeyWrap. The TOE provides key generation for AES 128-bit and 256-bit keys using a Random Number Generator that meets NIST SP 800-90 DRBG as specified in FIPS 140-2 Annex C. The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128, 256 bits) as described in FIPS PUB 197, "Advanced Encryption Standard (AES)" and NIST SP 800-38A. (Refer to FIPS 140-2 certificate #s 1942).
FCS_COP.1(4)	The TOE provides MD5 hashing for authentication of neighbor routers via BGPv4, EIGRP, EIGRPv6 for IPv6, RIPv2, and OSPFv2 with shared passwords. The hash mechanism is implemented as specified in the relevant RFCs: • BGPv4 uses MD5 for authentication of routing updates as defined in RFC 2385 (Protection of BGP Sessions via TCP MD5 Signature Option). • EIGRP and EIGRPv6 (Cisco proprietary) uses MD5 for authentication of routing updates. • RIPv2 uses MD5 for authentication of routing updates as defiend in Section 2.4 of RFC 2453. • OSPFv2 uses MD5 for authentication of routing updates as defined in Appendix D of RFC 2328 (OSPF version 2). Routing tables for IPv4 and IPv6 can be created and maintained manually using static routes configured by the administrator. Use of routing protocols in IPv4 or IPv6 is not required to support or enforce any TOE security functionality including filtering of IPv4 or IPv6 traffic. BGPv4, EIGRP and EIGRPv6 supports MD5-authenticated routing updates with IPv6 or IPv4 as does RIPv2 while OSPFv2 routing protocol support MD5-authenticated routing updates for IPv4 only. 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.
FCS_COP.1(5)	The TOE provides cryptographic hashing services using SHA-1 that meets FIPS Pub 180-3 "Secure Hash Standard".
FCS_COP.1(6)	The TOE uses HMAC-SHA1 message authentication that meets FIPS Pub 198-1 "The Keyed-Hash Message Authentication Code", and FIPS PUB 180-3,

TOE SFRs	How the SFR is Met
	"Secure Hash Standard".
FCS_SSH_EXT.1	The TOE implements SSHv2 (telnet is disabled in the evaluated configuration). SSHv2 sessions are limited to a configurable session timeout period of 120 seconds, a maximum number of failed authentication attempts limited to 3, and will be rekeyed upon request from the SSH client. SSH connections will be dropped if the TOE receives a packet larger than 35,000 bytes. The TOE's implementation of SSHv2 supports hashing algorithms hmac-sha1, hmac-sha1-96. The TOE can also be configured to use one of the identified DH groups for key exchange. The available groups include Diffie Hellmen group 14, group 16, and group 2.
FDP_IFC.1(1) FDP_IFF.1(1)	VLAN – A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. **VLANs have the same attributes as physical LANs**, but can group end stations even if they are not physically located on the same LAN segment. **Any switch port can belong to a VLAN**, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a switch supporting fallback bridging. In a switch stack, VLANs can be formed with ports across the stack. Because **a VLAN is considered a separate logical network**, it contains its own bridge Management Information Base (MIB) information The following diagram illustrates VLANs as Logically Defined Networks  **VLANs are often associated with IP subnetworks**. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch is assigned manually on an interface-by-interface basis. When an administrator assigns switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership. Traffic between VLANs must be routed or fallback bridged. The switch can route traffic between VLANs by using switch virtual interfaces (SVIs). PVLAN- **As with regular VLANs, private VLANs can span multiple switches**. A trunk port carries the primary VLAN and secondary VLANs to a neighboring switch. **The trunk port treats the private VLAN as any other VLAN. A feature of private VLANs across multiple switches is that traffic from an**

TOE SFRs	How the SFR is Met
	isolated port in switch A does not reach an isolated port on Switch B. See the diagram below Private VLANs across Switches  The TOE controls the flow of Ethernet traffic by matching VLAN tag information contained in the Ethernet frame headers against a set of rules specified by the authorized administrator in the VLAN flow control policies. **VLANs enforce separation of traffic that terminates at the TOE, as well as traffic flowing through the TOE. VLANs are also used to isolate the TOE's use of routing protocols for routing table updates, and the associated neighbor router authentication**. VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations. The VLAN SFP includes support for Private VLANs (PVLANs). **PVLANs partition a regular VLAN domain into subdomains**. A subdomain is represented by a pair of VLANs: a primary VLAN and a secondary VLAN. A PVLAN can have multiple VLAN pairs, one pair for each subdomain. In the following diagram there are two types of secondary VLANs illustrated: • Isolated VLANs—Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level. • Community VLANs—Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level. **PVLANs provide Layer 2 isolation between ports within the same PVLAN.**

TOE SFRs	How the SFR is Met
	PVLAN ports are access ports that are one of these types: • Promiscuous—A promiscuous port belongs to the primary VLAN and can communicate with all interfaces, including the community and isolated host ports that belong to the secondary VLANs associated with the primary VLAN. • Isolated—An isolated port is a host port that belongs to an isolated secondary VLAN. It has complete Layer 2 separation from other ports within the same private VLAN, except for the promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports. • Community—A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities and from isolated ports within their private VLAN.  Primary and secondary VLANs have these characteristics: • Primary VLAN—A PVLAN has only one primary VLAN. Every port in a PVLAN is a member of the primary VLAN. The primary VLAN carries unidirectional traffic downstream from the promiscuous ports to the (isolated and community) host ports and to other promiscuous ports. • Isolated VLAN —A PVLAN has only one isolated VLAN. An isolated VLAN is a secondary VLAN that carries unidirectional traffic

TOE SFRs	How the SFR is Met

upstream from the hosts toward the promiscuous ports and the gateway.

- Community VLAN—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. Multiple community VLANs can be configured in a PVLAN.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs.
PVLANs can be used to control access to end stations in these ways:

- Configure selected interfaces connected to end stations as isolated ports to prevent any communication at Layer 2. For example, if the end stations are servers, this configuration prevents Layer 2 communication between the servers.
- Configure interfaces connected to default gateways and selected end stations (for example, backup servers) as promiscuous ports to allow all end stations access to a default gateway.
- Extend PVLANs across multiple devices by trunking[8] the primary, isolated, and community VLANs to other devices that support PVLANs. To maintain the security of the PVLAN configuration and to avoid other use of the VLANs configured as PVLANs, configure PVLANs on all intermediate devices, including devices that have no PVLAN ports.

The following is an example showing how to configure and associating VLANS in a PVLAN. Begin in the privileged EXEC mode and follow the steps below. Note, the private-vlan commands do not take effect until the VLAN configuration mode is exited.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp mode transparent**	Set VTP mode to transparent (disable VTP).
Step 3	**vlan** *vlan-id*	Enter VLAN configuration mode and designate or create a VLAN that will be the primary VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.
Step 4	**private-vlan primary**	Designate the VLAN as the primary VLAN.
Step 5	**exit**	Return to global configuration mode.
Step 6	**vlan** *vlan-id*	(Optional) Enter VLAN configuration mode and designate or create a VLAN that will be an isolated VLAN. The

[8] Use of VLAN trunking (within the constraints described in section 1.8, "Excluded Functionality") is permitted in the evaluated configuration, and does not interfere with the TOE's inspection of VLAN tag information in frame headers, and proper forwarding or blocking based on that header inspection.

TOE SFRs	How the SFR is Met

		VLAN ID range is 2 to 1001 and 1006 to 4094.
Step 7	**private-vlan isolated**	Designate the VLAN as an isolated VLAN.
Step 8	**exit**	Return to global configuration mode.
Step 9	**vlan** *vlan-id*	(Optional) Enter VLAN configuration mode and designate or create a VLAN that will be a community VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.
Step 10	**private-vlan community**	Designate the VLAN as a community VLAN.
Step 11	**exit**	Return to global configuration mode.
Step 12	**vlan** *vlan-id*	Enter VLAN configuration mode for the primary VLAN designated in Step 2.
Step 13	**private-vlan association** [**add** | **remove**] *secondary_vlan_list*	Associate the secondary VLANs with the primary VLAN.
Step 14	**end**	Return to privileged EXEC mode.
Step 15	**show vlan private-vlan** [**type**] or **show interfaces status**	Verify the configuration.
Step 16	**copy running-config startup config**	Save your entries in the switch startup configuration file. To save the private-VLAN configuration, you need to save the VTP transparent mode configuration and private-VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it defaults to VTP server mode, which does not support private VLANs.

When you associate secondary VLANs with a primary VLAN, note this syntax information:

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- The *secondary_vlan_list* parameter can contain multiple community VLAN IDs but only one isolated VLAN ID.
- Enter a *secondary_vlan_list*, or use the **add** keyword with a *secondary_vlan_list* to associate secondary VLANs with a primary

TOE SFRs	How the SFR is Met
	VLAN. • Use the **remove** keyword with a *secondary_vlan_list* to clear the association between secondary VLANs and a primary VLAN. The following example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, and VLANs 502 and 503 as community VLANs, to associate them in a private VLAN, and to verify the configuration: Switch# **configure terminal** Switch(config)# **vlan 20** Switch(config-vlan)# **private-vlan primary** Switch(config-vlan)# **exit** Switch(config)# **vlan 501** Switch(config-vlan)# **private-vlan isolated** Switch(config-vlan)# **exit** Switch(config)# **vlan 502** Switch(config-vlan)# **private-vlan community** Switch(config-vlan)# **exit** Switch(config)# **vlan 503** Switch(config-vlan)# **private-vlan community** Switch(config-vlan)# **exit** Switch(config)# **vlan 20** Switch(config-vlan)# **private-vlan association 501-503** Switch(config-vlan)# **end** Switch(config)# **show vlan private vlan** Primary Secondary Type Ports ------- --------- ----------------- ---------------------- -------------------- 20 501 isolated 20 502 community

TOE SFRs	How the SFR is Met
	20 503 community 20 504 non-operational The following shows how to configure a Layer 2 interface as a PVLAN Host Port. Beginning in privileged EXEC mode, follow these steps to configure a Layer 2 interface as a private-VLAN host port and to associate it with primary and secondary VLANs, note the Isolated and community VLANs are both secondary VLANs. <table><tr><th></th><th>Command</th><th>Purpose</th></tr><tr><td>Step 1</td><td>configure terminal</td><td>Enter global configuration mode.</td></tr><tr><td>Step 2</td><td>interface interface-id</td><td>Enter interface configuration mode for the Layer 2 interface to be configured.</td></tr><tr><td>Step 3</td><td>switchport mode private-vlan host</td><td>Configure the Layer 2 port as a private-VLAN host port.</td></tr><tr><td>Step 4</td><td>switchport private-vlan host-association primary_vlan_id secondary_vlan_id</td><td>Associate the Layer 2 port with a private VLAN.</td></tr><tr><td>Step 5</td><td>end</td><td>Return to privileged EXEC mode.</td></tr><tr><td>Step 6</td><td>show interfaces [interface-id] switchport</td><td>Verify the configuration.</td></tr><tr><td>Step 7</td><td>copy running-config startup config</td><td>(Optional) Save your entries in the switch startup configuration file.</td></tr></table> This example shows how to configure an interface as a private-VLAN host port, associate it with a private-VLAN pair, and verify the configuration: Switch# **configure terminal** Switch(config)# **interface gigabitethernet1/0/22** Switch(config-if)# **switchport mode private-vlan host** Switch(config-if)# **switchport private-vlan host-association 20 501** Switch(config-if)# **end** Switch# **show interfaces gigabitethernet1/0/22 switchport** Name: Gi1/0/22 Switchport: Enabled

TOE SFRs	How the SFR is Met
	Administrative Mode: private-vlan host Operational Mode: private-vlan host Administrative Trunking Encapsulation: negotiate Operational Trunking Encapsulation: native Negotiation of Trunking: Off Access Mode VLAN: 1 (default) Trunking Native Mode VLAN: 1 (default) Administrative Native VLAN tagging: enabled Voice VLAN: none Administrative private-vlan host-association: 20 501 Administrative private-vlan mapping: none Administrative private-vlan trunk native VLAN: none Administrative private-vlan trunk Native VLAN tagging: enabled Administrative private-vlan trunk encapsulation: dot1q Administrative private-vlan trunk normal VLANs: none Administrative private-vlan trunk private VLANs: none Operational private-vlan: 20 501 The following shows Monitoring Private VLANs. Begin in the privileged EXEC mode and issue the commands for monitoring private-VLAN activity.

Command	Purpose
show interfaces status	Displays the status of interfaces, including the VLANs to which they belongs.
show vlan private-vlan [**type**]	Display the private-VLAN information for the switch or switch stack.
show interface switchport	Display private-VLAN configuration on interfaces.

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<table><tr><td>show interface private-vlan mapping</td><td>Display information about the private-VLAN mapping for VLAN SVIs.</td></tr></table>

The following is an example of the output from the show vlan private-vlan command:

Switch(config)# show vlan private-vlan

Primary Secondary Type Ports

------- --------- ----------------- --

10 501 isolated Gi2/0/1, Gi3/0/1, Gi3/0/2

10 502 community Gi2/0/11, Gi3/0/1, Gi3/0/4

10 503 non-operational
</td></tr>
<tr><td>FDP_IFC.1(2)
FDP_IFF.1(2)</td><td>The TOE controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator in the IP flow control policies. Within an ACL, the first entry in the ACL that matches the inspected traffic is the rule that’s applied. ACLs can be applied inbound to an interface and/or outbound from an interface. All ACLs applicable to a traffic flow through the TOE applied in the order in which they are encountered, i.e. any inbound ACL are applied to the traffic flow when the packet is received (after any Layer 2 VLAN SFP is applied) and any outbound ACL is applied before the packet is transmitted. For routed traffic, the outbound interface is determined by the routing table.

Use of routing protocols specified as permitted in the TOE description (BGPv4, EIGRP, EIGRPv6 for IPv6, RIPv2, and OSPFv2) does not interfere with the inspection of packets and proper enforcement of rules defined in FDP_IFF.1(2). Use of the routing table is required to determine the proper egress port for IP traffic flows, and thus which, if any, outbound ACL will be applied to the traffic flow, and static or dynamic updates to the routing table are expected and consistent with proper enforcement of traffic flow controls for Layer 3 traffic. Since routing tables are used to determine which egress ACL is applied, the authority to modify the routing tables is restricted to authenticated administrators, and authenticated neighbor routers.</td></tr>
<tr><td>FDP_IFC.1(3)
FDP_IFF.1(3)</td><td>Unlike regular Cisco IOS ACLs (discussed in FDP_IFF.1(2)) that are configured on Layer 3 interfaces only and are applied on routed packets only, VACLs apply to all packets and can be applied to any VLAN. As with ACLs for Layer 3 interfaces discussed in FDP_IFF.1(2), the TOE controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator in the IP flow control policies.
VACLs provide access control for packets that traverse the VLANs to which</td></tr>
</table>

TOE SFRs	How the SFR is Met
	VACLs are applied, whether bridged within a VLAN or routed into or out of a VLAN. o When a VACL is applied to a VLAN, all packets traversing a port in that VLAN are checked against this VACL. o When a VACL is applied to a VLAN, and an ACL is applied a routed interface in that VLAN, a packet entering the TOE through a port in the VLAN is first checked against the VACL, and, if permitted, is then checked against the inbound/ingress ACL applied to the routed interface per FDP_IFF.1(2). o You can set the action to drop, forward, forward capture, or redirect packets. o VACLs applied to WAN interfaces support only the forward capture action. VACLs applied to WAN interfaces do not support the drop, forward, or redirect actions. o Forwarded packets are still subject to any configured Cisco IOS security ACLs. o The capture action sets the capture bit for the forwarded packets so that ports with the capture function enabled can receive the packets. Only forwarded packets can be captured. Note, the port will need to be configured when this action is listed. . o VACLs applied to WAN interfaces do not support the log action. When the log action is specified, dropped packets are logged in software. Only dropped IP packets can be logged. o The redirect action allows you to specify up to five interfaces, which can be physical interfaces or EtherChannels. You cannot specify packets to be redirected to an EtherChannel member or a VLAN interface. o The redirect interface must be in the VLAN for which the VACL access map is configured. o Use the no keyword to remove an action clause or specified redirect interfaces. This example shows how to configure a Fast Ethernet interface 5/1 as a capture port: Router(config)# interface gigabitEthernet 5/1 Router(config-if)# switchport capture Router(config-if)# end Step 1 Router(config)# **interface** {{type1 slot/port} *specifies the interface to configure* Step 2 Router(config-if)# **switchport capture allowed vlan** {**add** | **all** | **except** | **remove**} *vlan_list* *(Optional) Filters the captured traffic on a per-destination-VLAN basis. The default is all.* Router(config-if)# **no switchport capture allowed vlan** *Clears the configured destination VLAN list and returns to the default value (all).* Step 3 Router(config-if)# **switchport capture** *Configures the port to capture VACL-filtered traffic.* Router(config-if)# **no switchport capture** *Disables the capture function on the interface.* You can configure a port as the capture port. However the capture port supports

TOE SFRs	How the SFR is Met
	only egress traffic and no traffic can enter the switch through a capture port. When the packet is routed within the TOE to another VLAN, it is first checked against the outbound/egress ACL applied to the routed interface per FDP_IFF.1(2), and, if permitted, is then checked against the VACL configured for the destination VLAN. For context of the above description, the following example shows how to identify and apply a VLAN access map *vmap4* to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list *al2*: Switch(config)# **vlan access-map vmap4** Switch(config-access-map)# **match ip address al2** Switch(config-access-map)# **action forward** Switch(config-access-map)# **exit** Switch(config)# **vlan filter vmap4 vlan-list 5-6**
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_ATD.1	The TOE maintains and manages the following user security attributes; user identity, privilege levels, and password. The user name and password are used by the TOE to identify and authenticate an administrator wishing to gain access to the TOE management functionality. The privilege level is used by the TOE to allow an authenticated user to assume a predefined TOE privilege level and perform specific management functions. For neighbor routers, which do not have access to the interactive admin interface, the attributes maintained are IP address and password, which are used to authenticate the remote router for exchange of routing table information.
FIA_UAU.2 FIA_UID.2	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through the TOE's CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE either through a directly connected console or remotely through an SSHv2 connection, the TOE prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. For neighbor routers, which do not have access to the CLI, the neighbor router must present the correct hashed password prior to exchanging routing table updates with the TOE. The TOE authenticates the neighbor router using its supplied password hash, and the source IP address from the IP packet header. The supported routing protocols (BGPv4, EIGRP, EIGRPv6 for IPv6, RIPv2, and OSPFv2) uses MD5 hashes to secure the passwords as specified in FCS_COP.1.1(4). Note, OSPFv2 also supports hmac-sha1 hases to secure the password. For additional security, router protocol traffic can also be isolated to separate VLANs.

TOE SFRs	How the SFR is Met
FIA_UAU.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, and authentication is performed implicitly through the supported protocols. 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.
FIA_UAU.7	When a user enters their password at the local console or via SSHv2, the TOE echoes none of the characters of the password.
FMT_MOF.1	The TOE provides the authorized administrative user the ability to perform the actions required to control the TOE, including: audit trail (create, delete, empty, review) management, network traffic (information flow) rules (create, delete, modify, and view), routing tables (create, modify, delete), session inactivity time period (set, modify threshold limits), time determination (set, change date/timestamp), and TSF self test (TOE and cryptographic module). For each of these functions that require data to be entered, only secure (authorized) values are accepted. Refer to the Guidance documentation for configuration syntax, commands, and information related to each of the functions. Some of the functions are restricted to a specific administrative privilege level and/or to an authorized administrator with the proper permissions (level).
FMT_MSA.2	The TOE inspects the headers of incoming frames and packets to ensure that the headers and the security-relevant information they contain, such as VLAN tags and addresses, is appropriately structured, and malformed frames and packets are discarded. The TOE's administrative interfaces only permit valid values to be specified within administratively-defined rules for the VLAN SFP, VACL SFP,ACL SFP, and PRIVAC SFP. For the VLAN SFP, the administrative interfaces ensure that the administrator will only be able to associate valid (configured) VLANs with valid (configured) Layer 2 (switch port) interfaces For the VACL SFP, the interfaces ensure that the administrator will only be able to associate valid (configured) VACLs that will be applied to packets that traverse the VLANs whether bridged within a VLAN or routed into or out of a VLAN. For the ACL SFP, the administrative interfaces will ensure that the administrator will only be able to associate a single outbound ACL, and/or a single inbound ACL on any one Layer 3 interface. Further, the administrative interface will ensure that only valid value formats are permitted for security relevant information and subject attributes in ACLs, including valid IP address formats, masks, protocol identifiers, and port numbers. For the PRIVAC SFP, the TOE ensures that only valid privilege levels and associated passwords are assigned. Guidance is also provided when assigning privilege levels to commands that contain more than word so that it is understood that privilege is being granted for all words at the level.
FMT_MSA.3(1)	The default TOE VLAN SFP, VACL SFP, and ACL SFP are permissive within

TOE SFRs	How the SFR is Met
	the TOE. The flow control policies must be administratively configured to be restrictive. When no VLANs or PVLANs have been explicitly created by the administrator and applied to ports, the ports are configured in a single default VLAN and thus traffic is allowed to flow among the ports. When no ACLs have been explicitly created and applied to interfaces, IP traffic is allowed to flow between subnets as defined in the routing table. The TOE only permits the authorized administrators to specify the flow control policies rules used to enforce the SFP through the administrative interface.
FMT_MSA.3(2)	The default TOE PRIVAC SFP is restrictive by default; with the exception of when the TOE is configured an administrator role is created. This is the Privileged administrator that is the equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15. When other administrators are configured, they must be assigned a privileged level prior to gaining access to the TOE and/or the CLI commands.
FMT_MTD.1	The TOE provides the ability for authorized administrators to access TOE data, such as audit data, configuration data, security attributes, information flow rules, routing tables, and session thresholds. Each of the predefined and administratively configured privilege level has a set of permissions that will grant them 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 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. 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, a terminal server, or at the local console. Refer to the Guidance documentation for configuration syntax, commands, and information related to each of these functions. 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, such as generating the RSA keys to enable SSHv2, configuration of routing protocols, and if used the configuration of remote authentication • Ability to manage the audit logs and functions - allows the authorized administrator to configure the audit logs, view the audit logs, and to clear the audit logs • Ability to manage information flow control attributes - allows the authorized administrator to configure the VLANs, PVLANS, and ACLs, to control the Ethernet and IP network traffic

TOE SFRs	How the SFR is Met
	• Ability to manage routing tables - allows the authorized administrator the ability to create, modify, and delete the routing tables to control the routed network traffic • Ability to manage security attributes belonging to individual users - allows the authorized administrator to create, modify, and delete other administrative users • Ability to manage the default values of the security attributes - allows the authorized administrator to specify the attributes that are used control access and/or manage users • Ability to manage the warning banner message and content – allows the authorized administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users • Ability to manage the time limits of session inactivity – allows the authorized administrator the ability to set and modify the inactivity time threshold
FDP_ACC.2/FDP_ACF.1 FMT_SMR.1	The TOE switch platform maintains administrative privilege level and non-administrative access. Non-administrative access is granted to authenticated neighbor routers for the ability to receive updated routing tables per the information flow rules. There is no other access or functions associated with non-administrative access. The administrative privilege levels include: • Administrators are assigned to privilege levels 0 and 1. Privilege levels 0 and 1 are defined by default and are customizable. These levels have a very limited scope and access to CLI commands that include basic functions such as login, show running system information, turn on/off privileged commands, logout. • Semi-privileged administrators equate to any privilege level that has a subset of the privileges assigned to level 15; levels 2-14. These levels are undefined by default and are customizable. The custom level privileges are explained in the example below. • Privileged administrators are equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15. Note, the levels are not hierarchical. For levels, level 0 is the most restrictive and 15 is the least restrictive. For level 0, there are five commands associated with privilege level 0: disable, enable, exit, help, and logout. However, the level could be configured to allow a user to have access to the ‘show’ command. Level 1 is normal EXEC-mode user privileges Following is an example of how privileges are set and rules in setting privilege levels and assigning users to those privilege levels. Note, that the administrator needs to have the appropriate privilege level and if required, applicable password to execute the command. When setting the privilege level for a command with multiple words

TOE SFRs	How the SFR is Met
	(commands), the commands starting with the first word will also have the specified access level. For example, if the **show ip route** command is set to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15—unless they are individually set to different levels. This is necessary because a user cannot execute, for example, the **show ip** command unless the user also has access to **show** commands. To change the privilege level of a group of commands, the **all** keyword is used. When a group of commands is set to a privilege level using the **all** keyword, all commands which match the beginning string are enabled for that level, and all commands which are available in submodes of that command are enabled for that level. For example, if the **show ip** keywords is set to level 5, **show** and **ip** will be changed to level 5 and all the options that follow the **show ip** string (such as **show ip accounting**, **show ip aliases**, **show ip bgp**, and so on) will be available at privilege level 5. The **privilege** command is used to move commands from one privilege level to another in order to create the additional levels of administration. The default configuration permits two types of users to access the CLI. The first type of user is a person who is only allowed to access user EXEC mode. The second type of user is a person who is allowed access to privileged EXEC mode. A user who is only allowed to access user EXEC mode is not allowed to view or change the configuration of the networking device, or to make any changes to the operational status of the networking device. On the other hand, a user who is allowed access to privileged EXEC mode can make any change to a networking device that is allowed by the CLI. Following is an example for setting the privilege levels for staff that are usually not allowed to run all of the commands available in privileged EXEC mode (privilege level 15) on a networking device. They are prevented from running commands that they are not authorized for by not being granted access to the password assigned to **privileged EXEC** mode or to other levels that have been configured on the networking device. The steps and commands show setting privilege level 7 with access to two commands, clear counters and reload. Step 1 **enable** password Enters privileged EXEC mode. Enter the password when prompted. Router> **enable** Step 2 **configure terminal** Enters global configuration mode. Router# **configure terminal** Step 3 **enable secret level** *level password* Configures a new enable secret password for privilege level 7. Router(config)# **enable secret level** *7 Zy72sKj* Step 4 **privilege exec level** *level command-string* Changes the privilege level of the clear counters command from privilege level 15 to privilege level 7. Router(config)# **privilege exec level** *7 clear counters* Step 5 **privilege exec all level** *level command-string* Changes the privilege level of the reload command

TOE SFRs	How the SFR is Met
	from privilege level 15 to privilege level 7. Router(config)# **privilege exec all level** *7 reload* Step 6 **end** Exits global configuration mode. Router(config)# **end** The following example shows the enforcement of the settings above and privilege levels. Step 1 **enable** *level password* Logs the user into the networking device at the privilege level specified for the level argument. Router> **enable** *7 Zy72sKj* Step 2 **show privilege** Displays the privilege level of the current CLI session Router# **show privilege** Current privilege level is 7 Step 3 **clear counters** The clear counters command clears the interface counters. This command has been changed from privilege level 15 to privilege level 7. Router# **clear counters** Clear "show interface" counters on all interfaces [confirm] Router# 02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console Step 4 **clear ip route** * The *ip route* argument string for the **clear** command should not be allowed because it was not changed from privilege level 15 to privilege level 7. Router# **clear ip route *** ^ % Invalid input detected at '^' marker. Router# Step 5 **reload in time** The reload command causes the networking device to reboot. Router# **reload in** *10* Reload scheduled in 10 minutes by console Proceed with reload? [confirm] Router# *** *** --- SHUTDOWN in 0:10:00 --- *** 02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20 Step 6 **reload cancel** The reload cancel terminates a reload that was previously setup with the reload in time command. Router# **reload cancel** *** *** --- SHUTDOWN ABORTED ---

TOE SFRs	How the SFR is Met
	*** 04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED: Scheduled reload cancelled at 15:38:46 PST Sun Mar 27 2005 Step 7 **disable** Exits the current privilege level and returns to privilege level 1. Router# **disable** Step 8 **show privilege** Displays the privilege level of the current CLI session Router> **show privilege** Current privilege level is 1 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 privilege level determines the functions the user can perform; hence the authorized administrator with the appropriate privileges. Refer to the Guidance documentation and IOS Command Reference Guide for available commands and associated roles and privilege levels. The Switch can and shall be configured to authenticate all access to the command line interface using a username and password.
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. For this TOE, the replay detection only applies to SSH protected communications (e.g. remote administrator encrypted sessions to the TOE). Note: The intended scope of this requirement is trusted (secure) communications with the TOE (e.g., administrator to TOE, IT entity (e.g., authentication server) to TOE, if that communications path is secure (use of SSHv2 or some other cryptographic protocol). 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 used in audit timestamps and in calculating session inactivity. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive clock updates from an NTP server. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions.
FPT_TST_EXT.1	As a FIPS 140-2 validated product, the TOE runs a suite of self-tests during initial start-up to verify its correct operation. Refer to the FIPS Security Policy for available options and management of the cryptographic self-test. For testing of the TSF, the TOE automatically runs checks and tests at startup and during resets to ensure the TOE is operating correctly. For the TSF self-test, successful completion of the self-test is indicated by reaching the log-on prompt as startup. If there are issues, the applicable audit record is generated and displayed on the console. Refer to the Guidance documentation for installation configuration settings and information and troubling shooting if issues are identified.

TOE SFRs	How the SFR is Met
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.

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. In addition, 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 identified in the SFRs 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 privilege level 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.

7.1 Rationale for TOE Security Objectives

Table 15: Threat/TOE Objectives/Organization Security Policy Mappings

	T.AUDIT_REVIEW	T.AUTHADMIN	T.MEDIATE	T.NOAUDIT	T.NOAUTH	T.NOMGT	T.UNAUTH_MGT_ACCESS	T.TIME	T.USER_DATA_REUSE	P.ACCESS BANNER
O.ACCESS_CONTROL					X	X	X			
O.ADMIN_ROLE		X								
O.AUDIT_GEN	X							X		
O.AUDIT_VIEW	X			X						
O.CFG_MANAGE						X				
O.IDAUTH							X			
O.MEDIATE			X							
O.SELFPRO					X	X	X			
O.STARTUP_TEST							X			
O.TIME								X		
O.DISPLAY_BANNER										X
O.RESIDUAL_INFORMATION_CLEARING									X	

Table 16: Threat/Organizing Security Policy/TOE and TOE Environment Objectives Rationale

Threat/Organization Security Policy	Rationale
T.AUDIT_REVIEW	Actions performed by users may not be known to the administrators due to actions not being recorded locally or remotely in a manner suitable for allow interpretation of the messages. The O.AUDIT_GEN objective requires that the TOE generate audit records. The O.AUDIT_VIEW requires the TOE to provide the Authorized administrator with the capability to view Audit data. These two objectives provide complete TOE coverage of the threat. The OE.AUDIT_REVIEW objective on the environment assists in covering this threat on the TOE by requiring that the administrator periodically check the audit record, and/or to configure the TOE to transmit audit records to a remote syslog server.
T.AUTHADMIN	A semi-privileged administrator may configure the system in an insecure manner (on purpose or accidentally) resulting in an insecure configuration setting on the TOE. The O.CFG_MANAGE objective requires that the TOE will provide management tools/applications for the administrator to manage its security functions, reducing the possibility for error. The O.ACCESS_CONTROL and O.ADMIN_ROLE objectives ensures that only authorized administrator, with the proper privilege level have access to the TOE management functions. The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. The combination of these objectives ensures the TOE provides the ability for only the authorized administrator, with the proper privilege level to gain access to and manage the TOE.
T.MEDIATE	An unauthorized entity may send impermissible information through the TOE which results in the exploitation of resources on the network. The O.MEDIATE security objective requires that all information that passes through the network is mediated by the TOE.
T.NOAUDIT	An unauthorized user modifies or destroys audit data. The O.AUDIT_VIEW objective requires that the TOE will provide only the authorized administrator the capability to review and clear the audit data.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE to disrupt operations of the TOE. The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. The O.ACCESS_CONTROL objective ensures that only authorized administrator have access to the TOE management functions.
T.NOMGT	The administrator is not able to manage the security functions of the TOE, resulting in the potential for the TOE configuration to compromise security objectives and policies. The O.CFG_MANAGE objective requires that the TOE will provide management tools/applications for the administrator to

Threat/Organization Security Policy	Rationale
	manage its security functions, reducing the possibility for error. The O.ACCESS_CONTROL objective ensures that only authorized administrator have access to the TOE management functions. The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. The combination of these objectives ensures the TOE provides the ability for only the authorized administrator to gain access to and manage the TOE.
T.UNAUTH_MGT_ACCESS	An unauthorized user gains management access to the TOE and views or changes the TOE security configuration. The O.ACCESS_CONTROL objective restricts access to the TOE management functions to authorized administrators. The O.IDAUTH objective requires a user to enter a unique identifier and authentication before management access is granted. The O.STARTUP_TEST objective performs initial tests upon system startup to ensure the integrity of the TOE security configuration and operations. The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.
T.TIME	An authorized administrator will not be able to determine the sequence of events in the audit trail because the audit records are not correctly time-stamped. Evidence of a compromise or malfunction of the TOE may go unnoticed or not be properly traceable if recorded events are not properly sequenced through application of correct timestamps. The O.TIME objective mitigates this threat by providing the accurate time to the TOE for use in the audit records (O.AUDIT_GEN).
T.USER_DATA_REUSE	User data that is temporarily retained by the TOE in the course of processing network traffic could be inadvertently re-used in sending network traffic to a destination other than intended by the sender of the original network traffic. This threat is countered by the security objective O.RESIDUAL_INFORMATION_CLEARING 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.
P.ACCESS_BANNER	This Organization Security Policy is addressed by the organizational security policy O.DISPLAY_BANNER to ensure an advisory notice and consent warning message regarding unauthorized use of the TOE is displayed before the session is established.

7.2 Rationale for the Security Objectives for the Environment

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 Security Target are mutually supportive and their combination meets the stated security objectives.

Table 17: Assumptions/Threat/TOE Environment Objectives Mappings

	A.NOEVIL	A.TRAIN_AUDIT	A.TRAIN_GUIDAN	A.LOCATE	A.CONFIDENTIALITY	A.INTEROPERABILITY	A.LOWEXP	T.AUDIT_REVIEW
OE.AUDIT_REVIEW		X						X
OE.NOEVIL	X							
OE.TRAIN_GUIDAN			X					
OE.LOCATE				X				
OE.CONFIDENTIALITY					X			
OE.INTEROPERABILITY						X		
OE.LOWEXP							X	

Table 18: Assumptions/Threat/TOE Environment Objectives Rationale

Assumption	Rationale
A.NOEVIL	All authorized administrators are assumed not evil and will not disrupt the operation of the TOE intentionally. The OE.NOEVIL objective ensures that authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error.
A.TRAIN_GUIDAN	Personnel will be trained in the appropriate use of the TOE to ensure security and will refer to all administrative guidance to ensure the correct operation of the TOE. The OE.TRAIN_GUIDAN objective ensures that authorized administrators will be trained in the appropriate use of the TOE to ensure security and will refer to all administrative guidance to ensure the correct operation of the TOE.
A.TRAIN_AUDIT	Administrators will be trained to periodically review audit logs to identify sources of concern. The OE.AUDIT_REVIEW objective ensures that the authorized administrators are trained to periodically review audit logs to identify sources of concern.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.LOCATE objective ensures the processing resources of the TOE will be located within

Assumption	Rationale
	controlled access facilities, which will prevent unauthorized physical access.
A.CONFIDENTIALITY	The hard copy documents and soft-copy representations that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to authorized administrators. Audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic. The OE.CONFIDENTIALITY objective ensures the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to authorized administrators, and audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic.
A.INTEROPERABILITY	The TOE will be able to function with the software and hardware of other vendors on the network. The OE.INTEROPERABILITY objective ensures that the TOE will be able to function with the software and hardware of other vendors on the network.
A.LOWEXP	The threat of malicious attacks aimed at exploiting the TOE is considered low. The OE.LOWEXP objective ensures that the threat of a malicious attack in the intended environment is considered low.

7.3 Rationale for TOE Security Functional Requirements

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 Security Target are mutually supportive and their combination meets the stated security objectives.

Table 19: TOE Security Objective to Security Functional Requirements Mappings

	O.ACCESS_CONTROL	O.ADMIN_ROLE	O.AUDIT_GEN	O.AUDIT_VIEW	O.CFG_MANAGE	O.IDAUTH	O.MEDIATE	O.SELFPRO	O.STARTUP_TEST	O.TIME	O.DISPLAY_BANNER	O.RESIDUAL_INFORMATION_CLEARING
FAU_GEN.1			X									
FAU_GEN.2			X									
FAU_SAR.1				X								
FAU_STG.1	X			X								
FCS_CKM.1(1)								X				
FCS_CKM.1(2)								X				
FCS_CKM.4								X				
FCS_COP.1(1)								X				
FCS_COP.1(2)								X				
FCS_COP.1(3)								X				
FCS_COP.1(4)								X				
FCS_COP.1(5)								X				
FCS_COP.1(6)								X				
FCS_SSH_EXT.1								X				
FDP_ACC.2	X	X			X			X				
FD_ACF.1	X	X			X			X				
FDP_IFC.1(1)							X					
FDP_IFC.1(2)							X					
FDP_IFC.1(3)							X					
FDP_IFF.1(1)							X					
FDP_IFF.1(2)							X					
FDP_IFF.1(3)							X					
FDP_RIP.2												X

FIA_ATD.1						X						
FIA_UAU.2						X						
FIA_UAU.5						X						
FIA_UAU.7						X						
FIA_UID.2						X						
FMT_MOF.1	X											
FMT_MSA.2								X				
FMT_MSA.3(1)(2)	X						X					
FMT_MTD.1	X											
FMT_SMF.1					X							
FMT_SMR.1	X				X							
FPT_RPL.1								X				
FPT_STM.1			X							X		
FPT_TST_EXT.1									X			
FTA_SSL.3	X				X	X		X				
FTA_TAB.1											X	

Table 20: TOE Security Objective to Security Functional Requirements Rationale

Objective	Rationale
O.ACCESS_CONTROL	The TOE will restrict access to the TOE Management functions to the Authorized administrators. The TOE is required to provide the ability to restrict the use of TOE management/administration/security functions to authorized administrators of the TOE. These functions are performed on the TOE by the authorized administrators [FMT_MOF.1]. Only authorized administrators of the TOE may modify TOE data [FMT_MTD.1] and and delete audit data stored locally on the TOE [FAU_STG.1]. The TOE must be able to recognize the administrative privilege level that exists for the TOE [FMT_SMR.1]. The TOE must allow the privileged administrator to specify alternate initial values when an object is created [FMT_MSA.3(2)]. The TOE ensures that all user actions resulting in the access to TOE security functions and configuration data are controlled. The TOE ensures that access to TOE security functions and configuration data is based on the assigned user privilege level. The SFR FTA_SSL.3 also meets this objective by terminating a session due to meeting/exceeding the inactivity time limit.
O.ADMIN_ROLE	The will provide administrator privilege levels to isolate administrative actions by configuring and assigning privilege levels [FMT_SMR.1], thus controlling access to the commands [FDP_ACC.2/FDP_ACF.1]. The TOE will also make the administrative functions available locally and remotely.
O.AUDIT_GEN	The TOE will generate audit records which will include the time that the event occurred and if applicable, the identity of the user performing the event. Security relevant events must be defined and

Objective	Rationale
	auditable for the TOE [FAU_GEN.1 and FAU_GEN.2]. Timestamps associated with the audit record must be reliable [FPT_STM.1].
O.AUDIT_VIEW	The TOE will provide the authorized administrators the capability to review Audit data. Security relevant events must be available for review by authorized administrators [FAU_SAR.1]. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to delete audit data stored locally on the TOE [FAU_STG.1].
O.CFG_MANAGE	The TOE will provide management tools/applications to allow authorized administrators to manage its security functions. The TOE is capable of performing numerous management functions including the ability to manage the cryptographic functionality, to manage the audit logs and functions, to manage information flow control attributes, to manage security attributes that allows authorized administrators to manage the specified security attributes, to manage the default values of the security attributes, to initiate TOE self test, to manage the warning banner message and content, and to manage the time limits of session inactivity [FMT_SMF.1]. The TOE must be able to recognize the administrative roles that exist for the TOE [FMT_SMR.1] and [FDP_ACC.2/FDP_ACF.1] ensures the access to the commands is controlled and only those users (administrators) assigned the appropriate privilege can execute the command. FTA_SSL.3 also meets this objective by terminating a session due to meeting/exceeding the inactivity time limit. The TOE requires that all users, switches, devices and hosts actions resulting in the access to TOE security functions and configuration data are controlled to prevent unauthorized activity. The TOE ensures that access to TOE security functions and configuration data is done in accordance with the rules of the access control policy.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access. The TOE is required to provide users with security attributes to enforce the authentication policy of the TOE and to associate security attributes with users [FIA_ATD.1]. Users authorized to access the TOE must be defined using an identification and authentication process [FIA_UAU.5]. Before access is granted, all users must be successfully identified and authenticated [FIA_UID.2 and FIA_UAU.2]. The password is obscured when entered [FIA_UAU.7]. If the period of inactivity has been exceeded, the user is required to re-authenticate to re-establish the session [FTA_SSL.3].
O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE. The TOE is required to identify the subject attributes and information attributes necessary to enforce the VLAN information flow control SFP, and IP information flow control SFP [FDP_IFC.1(1), (2), (3) and FDP_IFF.1(1), (2), (3)]. The policy is defined by rules defining the conditions for which information is permitted or denied to flow [FDP_IFF.1(1),(2), (3)]. The TOE provided the capability for administrators to define default deny rules, though the default policy for the information flow control security rules is permissive where no explicit rules exist until created and applied by an authorized administrator [FMT_MSA.3].
O.SELFPRO	The TOE must protect itself against attempts by unauthorized users

Objective	Rationale
	to bypass, deactivate, or tamper with TOE security functions. [FDP_ACC.2/FDP_ACF.1] supports this objective by ensuring access to the commands is controlled and only those users (administrators) assigned the appropriate privilege can execute the command, and as such the administrators must be assigned a privilege level prior to gaining access to the TOE and/or the CLI commands [FMT_MSA.3(2)]. The switch component of the TOE provides an encrypted mechanism for remote management of the TOE and for protection of authentication data transferred between the switch and endpoints are secure by implementing the encryption protocols as defined in the SFRs and as specified by the RFCs, [FCS_COP.1(1), (2), (3), (4), (5), and (6), FCS_CKM.1(1) and (2), FCS_CKM.4, FCS_SSH_EXT.1, FMT_MSA.2]. The SFR FTA_SSL.3 also meets this objective by terminating a session due to meeting/exceeding the inactivity time limit thus ensuring the session does not remain active and subject to attack. FTP_RPL supports this objective by leveraging the ability of SSHv2 to terminate sessions when information replay is detected.
0.STARTUP_TEST	The TOE will perform initial startup tests upon bootup of the system. The TOE is required to demonstrate the correct operation of the security assumptions on startup by running initialization tests [FPT_TST_EXP.1].
O.TIME	The TSF will provide a reliable time stamp for its own use. The TOE is required to provide reliable timestamps for use with the audit record. [FPT_STM.1].
O.DISPLAY_BANNER	The TSF shall display a banner, before the user establishes a session. The SFR, FTA_TAB.1 meets this objective by displaying an advisory notice and consent warning message regarding unauthorized use of the TOE.
O.RESIDUAL_INFORMATION_CLEARING	The TOE must ensure that previous data are zeroized/overwritten so that the area used by a packet and then reused, data from the previous transmission does not make its way into a new packet transmission. 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.

ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 21: 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