Security Target

Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers

ST Version 1.4

August 17, 2009

Prepared For:

Force10 Networks, Inc.
350 Holger Way
San Jose CA 95134-1370
www.force10networks.com

Prepared By:

Apex Assurance Group, LLC
5448 Apex Peakway Drive, Ste. 101
Apex, NC 27502
www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers. 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.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers
ST Revision	1.4
ST Publication Date	August 17, 2009
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE

SECTION	TITLE	DESCRIPTION
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets and by a change in text color (Example: [assignment_value(s)]).
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

Italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
ACL	Access Control List
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
FTOS	Force10 Operating System
OSP	Organizational Security Policy
PBR	Policy Based Routing

TERM	DEFINITION
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

Table 2 – Acronyms Used in Security Target

1.6 TOE Overview and Description

1.6.1 Summary

The TOE platforms are hardware devices, and all TOE platforms run the Force10 Operating System (FTOS). This software provides management functions and switching/routing functionality (where applicable). Additionally, the version of FTOS is consistent across all of the following platforms:

- The Force10 Networks C-Series are resilient chassis-based switches that deliver reliability, network control and scalability. The C-Series is designed to support mission critical applications with very low latency across converged networks. Comprehensive management capabilities make the C-Series a cost-effective and flexible deployment option.

- The Force10 E-Series switch/routers provide best-in-class resiliency, unmatched scalability, line-rate performance, and full Layer 2 switching and Layer 3 routing. Based on revolutionary system architecture that combines fully distributed hardware and modular software, the E-Series switch/routers ensure predictable application performance, increase network availability, and reduce operating costs.

- The Force10 S-Series is a family of resilient, small form factor Gigabit and 10 Gigabit Ethernet switches designed to exceed requirements for enterprises and service providers alike. S-Series switches complement the resiliency and density of the Force10 E-Series, providing a scalable, high performance end-to-end network solution

Switching/routing functionality is managed by FTOS via local terminal console or via remote network session. To configure the TOE, an operator must first authenticate via username/password. Once authenticated, that operator will only have access to features and functions allowed by their privilege level, which is defined by an administrator.

The TOE boundaries for each product series are shown below (note that TOE components are shaded):

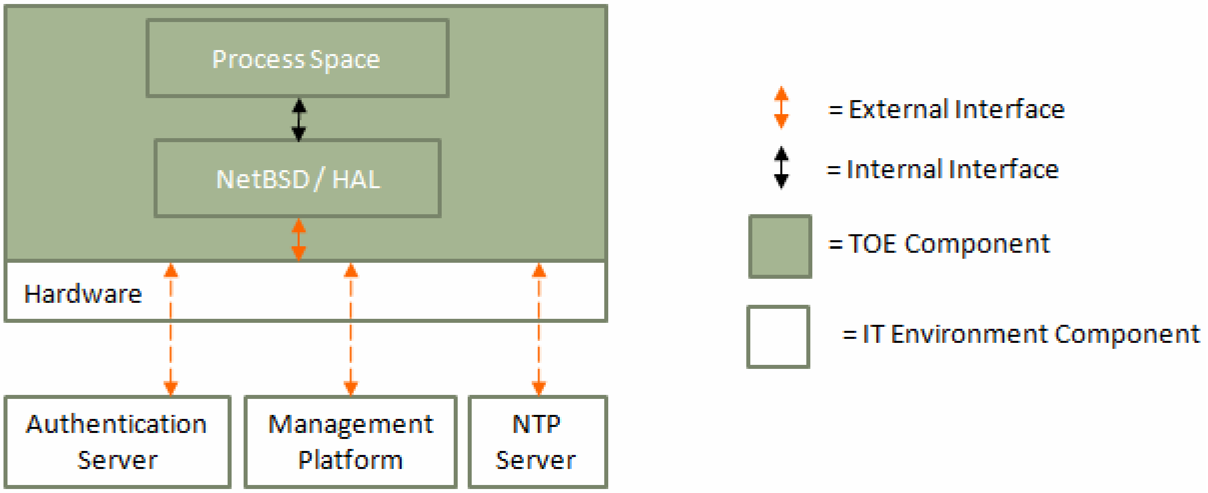

Figure 1 – TOE Boundary

1.6.2 Physical Boundary

The TOE is a software TOE and is defined as the FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers. In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Force10 Operating System Version 7.8.1.0
TOE Hardware (IT Environment)	C150, C300
	E300, E600, E1200
	S25N, S25P, S50N, S50V, S2410

Table 3 – Evaluated Configuration for the TOE

The TOE interfaces are comprised of the following:

1. Network interfaces which pass traffic (once processed by the Process Space)
2. Management interface through which handle administrative actions.

1.6.3 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

At a high level, the logical boundaries of the TOE are the functions of the TOE interfaces, including audit of security functions, control of traffic flow, authentication for the administrative functions, and the management of the security configurations.

TSF	DESCRIPTION
Security Audit	The TOE provides an audit feature for actions related to operator authentication attempts and administrator actions.
Identification and Authentication	Authentication services can be handled either internally (fixed passwords) or through an external authentication service, such as a RADIUS or TACACS+ server. An operator's authentication parameters must be valid before access is granted to administrative functions.
Information Flow Control	The TOE provides an Information Flow Control mechanism that supports control of the flow of traffic generated by the network devices. The Information Flow Control Policies are configured on each network devices to allow traffic to only flow between the authorized sources and authorized destinations.
Security Management	The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to Security Audit and Information Flow Control. Administrators configure the TOE via local CLI, telnet, or SNMP.

Table 4 – Logical Boundary Descriptions

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 2 (September 2007) Part 2 and Part 3 conformant at Evaluation Assurance Level 2.

2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE claims conformance to the assurance package defined by EAL2.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The TOE is targeted at a generalized IT environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have a Basic attack potential (as described in the Common Evaluation Methodology), and the assumed level of expertise of the attacker for all the threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.NO_AUDIT	An operator's attempt to violate TOE authentication and security management features may go undetected.
T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration.
T.NO_PRIVILEGE	An authorized user of the TOE exceeds his/her assigned security privileges resulting in the illegal modification of the TOE configuration and/or data.
T.TRAFFIC_FLOW	A user might be able to access information or network resources that should be restricted.

Table 5 – Threats

3.2 Organizational Security Policies

No Organizational Security Policies are identified for the TOE.

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.INSTALL	The TOE will be installed in a network infrastructure such that it can effectively control the flow of the applicable information.
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
A.REMOTE_AUTH	External authentication services will be available via either RADIUS, TACACS+, or both.
A.TIME	External NTP services will be available.

Table 6 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.AUDIT	The TOE shall record the necessary events to provide information operator authentication/actions and status of TOE interfaces.
O.MANAGE	The TOE must provide services that allow effective management of its functions and data.
O.SECURE_ACCESS	The TOE shall ensure that only those authorized users and applications are granted access to the security functions, configuration and associated data.
O.TRAFFIC_FLOW	The TOE shall control the flow of information among its network connections.

Table 7 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ADMIN	Authorized users must follow all administrator guidance
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
OE.REMOTE_AUTH	External authentication services will be available via TACACS+ and RADIUS.
OE.TIME	NTP server(s) will be available to provide accurate/synchronized time services to the router.

Table 8 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable).

OBJECTIVE THREATS/ ASSUMPTION	O.AUDIT	O.MANAGE	O.SECURE_ACCESS	O.TRAFFIC_FLOW	OE_ADMIN	OE.PHYSICAL	OE.REMOTE_AUTH	OE.TIME
A.INSTALL						✓		

OBJECTIVE THREATS/ ASSUMPTION	O.AUDIT	O.MANAGE	O.SECURE_ACCESS	O.TRAFFIC_FLOW	OE_ADMIN	OE.PHYSICAL	OE.REMOTE_AUTH	OE.TIME
A.NO_EVIL	✓				✓			
A.PHYSICAL						✓		
A.REMOTE_AUTH							✓	
A.TIME								✓
T.NO_AUDIT	✓							
T.NO_AUTH	✓		✓					
T.NO_PRIVILEGE	✓	✓	✓					
T.TRAFFIC_FLOW		✓		✓				

Table 9 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1.1 Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.NO_AUDIT	• O.AUDIT directly counters this threat by ensuring users are accountable for their actions in administering the TOE.
T.NO_AUTH	• O.SECURE_ACCESS directly counters this threat by ensuring that the TOE only allows authorized users and processes (applications) to access protected TOE functions and data. • O.AUDIT directly counters this threat by ensuring that users are accountable for their actions in administering the TOE.
T.NO_PRIVILEGE	• O.SECURE_ACCESS directly counters this threat by ensuring that the TOE only allows authorized users and processes (applications) to access protected TOE functions and data. • O.MANAGE directly counters this threat by ensuring that that the TOE management functions are accessible only by authorized users. • O.AUDIT directly counters this threat by ensuring that users are accountable for their actions in administering the TOE.
T.TRAFFIC_FLOW	• O.TRAFFIC_FLOW directly counters this threat by ensuring that that network packets flow from source to destination according to available routing information in the TOE configuration. • O.MANAGE directly counters this threat by ensuring authorized configuration of traffic routing.
A.INSTALL	• OE.PHYSICAL upholds this assumption by providing physical protection for the TOE

THREAT	RATIONALE
A.NO_EVIL	• O.AUDIT upholds this assumption by recording actions of users • OE.ADMIN upholds this assumption by claiming users should follow administrator guidance supports the assumption that they will not be careless, willfully negligent or hostile
A.PHYSICAL	• OE.PHYSICAL upholds this assumption by providing physical protection for the TOE
A.REMOTE_AUTH	• OE.REMOTE_AUTH upholds this assumption by providing authentication services via either RADIUS, TACACS+, or both.
A.TIME	• OE.TIME upholds this assumption by allowing use of an NTP server in the TOE environment

Table 10 – Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Definition of Extended Components

The TOE does not include extended components.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.1	Timing of Authentication
	FIA_UID.1	Timing of Identification
Information Flow Control	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 11 – TOE Security Objectives

6.1.1 Security Audit (FAU)

6.1.1.1 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:

- Start-up and shutdown of the audit functions;
- All auditable events for the not specified level of audit; and
- [operator authentication attempts and administrator actions].

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no additional information].

6.1.2 Information Flow Control (FDP)

6.1.2.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [information flow control SFP] on

[Subjects: IT entities that send information through the TOE,

Information: network traffic, and

Operations: switching and routing of information

].

6.1.2.2 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [information flow control SFP] based on the following types of subject and information security attributes:

[Subject security attributes:

- address

Information security attributes:

- IP address of the forwarding router (next-hop IP address)
- Protocol as defined in the header
- Source IP address and mask
- Destination IP address and mask
- Source port
- Destination port
- TCP Flags

].

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

[

- For switch and switch router configurations, information is allowed to flow between TOE interfaces only if:
  - a virtual circuit has been established between the inbound TOE interface and some other interface (in which case the information is forwarded to the associated outbound TOE interface) OR
  - the presumed destination address of the information identifies a subject associated with an outbound TOE interface (in which case the information is forwarded to the identified outbound TOE interface) OR
  - the presumed destination address of the information identifies a subject that is not associated with any TOE interface AND the TOE has been configured to broadcast traffic when it doesn't recognized the presumed address of the destination subject (in which case the information is broadcast out all TOE interfaces that are not configured as part of a virtual circuit).
- For switch router configurations the following ADDITIONAL rules are applied such that information is allowed to flow between TOE interfaces only if:
  - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator.

].

FDP_IFF.1.3 The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [no additional information flow control SFP rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [no additional information flow control SFP rules].

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Authentication Data, Privilege Level].

6.1.3.2 FIA_UAU.1 – Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [no administrative actions and information flow subject to the Information Flow SFP] on behalf of the user to be performed before the user is authenticated.

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

6.1.3.3 FIA_UID.1 – Timing of Identification

FIA_UID.1.1 The TSF shall allow [no administrative actions and information flow subject to the Information Flow SFP] on behalf of the user to be performed before the user is identified.

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

6.1.4 Security Management

6.1.4.1 FMT_MOF.1 – Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to *enable*, *disable*, *determine* and *modify the behavior of* the functions [the Information Flow Control SFP Rules and operator privileges] to [authorized administrator].

6.1.4.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [Information Flow Control SFP] to restrict the ability to *change_default*, *query*, *modify*, *delete*, and [no other operations] the security attributes [ACLs on the TOE] to [authorized administrators].

6.1.4.3 FMT_MSA.3 – Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Information Flow Control SFP] to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [authorized administrators] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.4 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default*, *query*, *modify*, *delete*, and [create] the [TOE configurations and operator account data] to [authorized administrators].

6.1.4.5 FMT_SMF.1 – Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [Manage Information Flow Control SFP and operator accounts].

6.1.4.6 FMT_SMR.1 – Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [authorized administrators].

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

6.2 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-Enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 12 – Security Assurance Requirements at EAL2

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE SFR	O.TRAFFIC_FLOW	O.MANAGE	O.SECURE_ACCESS	O.AUDIT
FAU_GEN.1				✓
FDP_IFC.1	✓			
FDP_IFF.1	✓			
FIA_ATD.1		✓	✓	✓
FIA_UAU.1		✓	✓	
FIA_UID.1		✓	✓	
FMT_MOF.1		✓	✓	
FMT_MSA.1	✓	✓		
FMT_MSA.2	✓	✓		
FMT_MSA.3	✓	✓		
FMT_MTD.1	✓	✓	✓	✓
FMT_SMF.1	✓	✓	✓	✓
FMT_SMR.1	✓	✓	✓	✓
FPT_STM.1				✓

Table 13 – Mapping of TOE Security Functional Requirements and Objectives

6.3.2 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

SFR	RATIONALE
FAU_GEN.1	This component outlines what events must be audited, and aids in meeting O.AUDIT.
FDP_IFC.1	This component identifies the entities involved in the Information Flow Control SFP (i.e. external IT entities sending packets), and aids in meeting O.TRAFFIC_FLOW.

SFR	RATIONALE
FDP_IFF.1	This component identifies the conditions under which information is permitted to flow between entities (the Information Flow Control SFP), and aids in meeting O.TRAFFIC_FLOW.
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. The component aids in meeting O.MANAGE, O.SECURE_ACCESS and O.AUDIT.
FIA_UAU.1	This component ensures that users are authenticated to the TOE. As such it aids in meeting objectives to restrict access (O.MANAGE and O.SECURE_ACCESS).
FIA_UID.1	This component ensures that users are identified to the TOE. As such it aids in meeting objectives to restrict access (O.MANAGE and O.SECURE_ACCESS).

SFR	RATIONALE
FMT_MOF.1	This component relates to control of the functions that address identification and authentication (local or RADIUS/TACACS+), and as such aids in meeting O.MANAGE and O.SECURE_ACCESS.
FMT_MSA.1	This component restricts the ability to modify, delete, or query the parameters for the Information Flow Control SFP to an authorized administrator, and as such aids in meeting O.TRAFFIC_FLOW, It also assists in effective management, and as such aids in meeting O.MANAGE.
FMT_MSA.2	This component ensures that only secure values are accepted for the configuration parameters associated with the Information Flow Control SFP, and as such aids in meeting O.TRAFFIC_FLOW. It also assists in effective management, and as such aids in meeting O.MANAGE.
FMT_MSA.3	This component ensures that there is a *default deny* policy for the information flow control security rules. As such it aids in meeting O.TRAFFIC_FLOW. It also assists in effective management, and as such aids in meeting O.MANAGE.
FMT_MTD.1	This component restricts the ability to modify the Information Flow Control SFP, and as such aids in meeting O.TRAFFIC_FLOW, O.MANAGE. This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.MANAGE and O.SECURE_ACCESS. This component restricts the ability to delete audit logs, and as such contributes to meeting O.AUDIT and O.MANAGE. This component restricts the ability to modify the date and time, and as such contributes to meeting O.AUDIT and O.MANAGE. This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.MANAGE.
FMT_SMF.1	This component lists the security management functions that must be controlled. As such it aids in meeting O.TRAFFIC_FLOW, O.MANAGE, O.SECURE_ACCESS, and O.AUDIT.
FMT_SMR.1	Each of the components in the FMT class listed above relies on this component (apart from FMT_MSA.3). It defines the roles on which access decisions are based. As such it aids in meeting O.TRAFFIC_FLOW, O.MANAGE, O.SECURE_ACCESS, and O.AUDIT.
FPT_STM.1	This component ensures that reliable time stamps are provided for audit records and aids in meeting O.AUDIT.

Table 14 – Rationale for TOE SFRs to Objectives

The following table presents a mapping of the rationale of TOE Objectives to Security Requirements:

OBJECTIVE	RATIONALE
O.SECURE_ACCESS	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. • FIA_UAU.1 which ensures that users are authenticated to the TOE. • FIA_UID.1 which ensures that users are identified to the TOE. • FMT_MOF.1 which relates to control of the functions that address detected security violations. • FMT_MTD.1 which restricts the ability to modify identification and authentication data • FMT_SMF.1 which lists the security management functions that must be controlled. • FMT_SMR.1 which defines the roles on which access decisions are based.
O.MANAGE	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. • FIA_UAU.1 which ensures that appropriate authentication mechanisms can be selected. • FIA_UID.1 which ensures that users are identified to the TOE. • FMT_MSA.1 assists in providing effective management of the TOE. • FMT_MSA.2 assists in providing effective management of the TOE. • FMT_MSA.3 assists in providing effective management of the TOE. • FMT_MOF.1 which relates to control of the functions that address detected security violations. • FMT_MTD.1 which restricts the ability to modify the Information Flow Control SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, and restricts the ability to modify the data relating to TOE access locations • FMT_SMF.1 which lists the security management functions that must be controlled. • FMT_SMR.1 which defines the roles on which access decisions are based.

OBJECTIVE	RATIONALE
O.AUDIT	This objective is completely satisfied by • FAU_GEN.1 which outlines what events must be audited. • FIA_ATD.1 which provides users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. • FMT_MTD.1 restricts the ability to delete audit logs and restricts the ability to modify the date and time. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based. • FPT_STM.1 ensures that reliable time stamps are provided for audit records.
O.TRAFFIC_FLOW	This objective is completely satisfied by • FDP_IFC.1 identifies the entities involved in the Information Flow Control SFP (i.e. external IT entities sending packets). • FDP_IFF.1 identifies the conditions under which information is permitted to flow between entities (the Information Flow Control SFP). • FMT_MSA.1 restricts the ability to modify, delete, or query the parameters for the Information Flow Control SFP to an authorized administrator • FMT_MSA.2 ensures that only secure values are accepted for the configuration parameters associated with the Information Flow Control SFP. • FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based.

Table 15 – Rationale for TOE Objectives to SFRs

6.3.3 Dependency of Security Functional Requirements

The following table presents a mapping of the TOE Security Requirements dependencies:

SFR	DEPENDENCY	SATISFIED
FAU_GEN.1	FPT_STM.1	✓
FDP_IFC.1	FDP_IFF.1	✓
FDP_IFF.1	FDP_IFC.1	✓
	FMT_MSA.3	✓
FIA_ATD.1	None	Not applicable
FIA_UAU.1	FIA_UID.1	✓
FIA_UID.1	None	Not applicable

SFR	DEPENDENCY	SATISFIED
FMT_MOF.1	FMT_SMF.1	✓
	FMT_SMR.1	✓
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Met by FDP_IFC.1
	FMT_SMF.1	✓
	FMT_SMR.1	✓
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1	Met by FDP_IFC.1
	FMT_MSA.1	✓
	FMT_SMR.1	✓
FMT_MSA.3	FMT_MSA.1	✓
	FMT_SMR.1	✓
FMT_MTD.1	FMT_SMF.1	✓
	FMT_SMR.1	✓
FMT_SMF.1	None	Not applicable
FMT_SMR.1	FIA_UID.1	✓
FPT_STM.1	None	Not applicable

Table 16 – SFR Dependencies

6.3.4 Security Assurance Requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers
ADV_TDS.1: Basic Design	Basic Design: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers
ALC_DEL.1: Delivery Procedures	Delivery Procedures: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers
ATE_COV.1: Evidence of Coverage	Security Testing: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers
ATE_FUN.1: Functional Testing	Security Testing: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers
ATE_IND.2: Independent Testing – Sample	Security Testing: Force10 Networks FTOS 7.8 for C-Series Switches, S-Series Switches, and E-Series Switch/Routers

Table 17 – Security Assurance Rationale and Measures

7 TOE Summary Specification

7.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 6.1 – Security Functional Requirements. The security functions performed by the TOE are as follows:

- Security Audit
- Identification and Authentication
- Information Flow Control
- Security Management

7.2 Security Audit

The Security Audit function provides auditing for user logon attempts, administrator actions, and status of interfaces. Logging functionality in the TOE is always enabled, and audit records include the following:

- Event time and date
- Event type
- Subject identity
- Outcome (e.g., success/failure).

The Security Audit security function is designed to satisfy the following security functional requirements:

- FAU_GEN.1

7.3 Identification and Authentication

The TOE requires operators to provide identification and authentication data (usernames and passwords, respectively) before any administrative actions can be performed. Authentication data can be stored locally or on a separate server supporting either the RADIUS or TACACS+ protocol.

If performing local authentication, the TOE will verify the username/password credentials entered by the operator. If valid, the operator has access to the functions defined by the respective privilege level. If the TOE is configured to work with a remote authentication server, the username and password is provided to the server, and the server returns a valid/invalid response. The TOE enforces this result; if valid, the operator will have access to features defined by their privilege level. In invalid, no administrative features are exposed.

This function ensures that operators are identified and authenticated before they can access any TSF-mediated functions in the TOE that are not associated with execution of information flow control policies.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1
- FIA_UAU.1
- FIA_UID.1

7.4 Information Flow Control

The Information Flow Control security function implements an information flow security policy that controls how information moves through the system and regulates exchange of information between devices connected to the TOE environment. This policy, enforced in all hardware platforms, associates subjects (based on their presumed source address) with TOE interfaces when traffic is received from those subjects.

Upon receipt of network traffic, the TOE will inspect the destination address, associate an outbound interface, then send the traffic to that interface. If no interface is associated, the traffic will be discarded or broadcast to all interfaces as defined by the TOE configuration.

The E Series switch/routers support the basic switch policies described above and also support more robust content filtering via Access Control Lists. Policy-Based Routing (PBR) enables an administrator to apply routing policies to a specific interface. The following parameters can be defined in the routing policies or rules:

- IP address of the forwarding router (next-hop IP address)
- Protocol as defined in the header
- Source IP address and mask
- Destination IP address and mask
- Source port
- Destination port
- TCP Flags

The rules for the Information Flow Control policy allow traffic to flow in broadcast mode by default (to facilitate deployment into a new environment). This is configurable by the administrator. Additionally, the switch/router E Series platforms can be configured with access control lists to define more specific traffic filters, allowing information flow control policy definition based on the following parameters: interfaces, source addresses, and destination addresses.

The Information Flow Control security function is designed to satisfy the following security functional requirements:

- FDP_IFC.1
- FDP_IFF.1

7.5 Security Management

The TOE provides the ability to manage user data (including authentication data, roles, etc.) and the information flow control policy (including ACLs). All security function management is handled through the local console, telnet, or SNMP, and management is restricted only to authorized administrators.

The Security Management security function provides interfaces for the appropriate management of the TOE information flow control policy. As discussed in the Information Flow Control section, the TOE bypasses information flow control restrictions; only an authorized administrator can change the initial default settings.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1
- FMT_MSA.1
- FMT_MSA.3
- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1