# Alcatel-Lucent OmniSwitch 9000E, 6855, 6850E, 6400 with AOS 6.4.4

## Security Target – EAL2

Release Date: December 19, 2011
Document ID: 011756-00
Version: 1.00 (Agile Rev.C)

Prepared By: InfoGard Laboratories

Prepared For: Alcatel-Lucent
26801 West Agoura Road,
Calabasas, CA 91301

# Table of Contents

# List of Tables



# List of Figures

# 1 Introduction

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

## 1.1 Identification

| | |
|---|---|
| TOE Identification: | Alcatel-Lucent OmniSwitch 9000E Series with AOS Release 6.4.4 |
| | Alcatel-Lucent Omniswitch 6855 Series with AOS Release 6.4.4 |
| | Alcatel-Lucent OmniSwitch 6850E Series with AOS Release 6.4.4 |
| | Alcatel-Lucent OmniSwitch 6400 Series with AOS Release 6.4.4 |
| ST Identification: | Alcatel-Lucent OmniSwitches 9000E, 6855, 6850E, 6400 with AOS 6.4.4 |
| ST Version: | 1.00 |
| ST Publish Date: | December 19, 2011 |
| ST Authors: | InfoGard Laboratories |

## 1.2 Overview

The TOE is a network switch that provides Layer-2 switching, Layer-3 routing, and traffic filtering. Layer-2 switches analyze incoming frames and makes forwarding decisions based on information contained in the frames. Layer-3 routing determines the next network point to which a packet should be forwarded toward its destination. These devices may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Routing protocols include BGP, RIP v.2, and OSPF. Filtering controls network traffic by controlling whether packets are forwarded or blocked at the switch's interfaces. Each packet is examined to determine whether to forward or drop the packet, on the basis of the criteria specified within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

The Alcatel OmniSwitch 6400 Series switches are fixed configuration stackable Gigabit Ethernet switches (10/100/1000). They provide advanced Layer-2 and basic routing capabilities.

The Alcatel OmniSwitch 6850E and 6855 series switches are fixed configuration, triple-speed (10/100/1000) Ethernet switches. They provide wire rate Layer-2 forwarding and Layer-3 routing with 10 Gig support. The 6850E series are either stand alone or stackable switches. The OmniSwitch 6855 series are hardened[1] Gigabit Ethernet fixed configuration switches that provide Layer-2 and Layer-3 switching only for use in harsh environmental conditions.

The Alcatel OmniSwitch 9000E (OS9000E) switches are comprised of the 9800E and 9700E models and are high performance switches for use in datacenters and campus networks. The OS9000E switches are chassis / blade systems. For example, the OS9800E switch is an 18 slot chassis, supporting two CMMs and 16 NI modules.

AOS release 6.4.4 is the single purpose operating system that operates the management functions of all of the Alcatel OmniSwitch switches.

## 1.3 Architecture Description

The main distinctions between the hardware models are the form factor (e.g., chassis or stacks), number

[1] The term hardened in this document refers to industrial, ruggedized equipment that is designed to operate in harsh electrical conditions and at extreme temperatures, vibration, noise, etc.

and type of physical ports and the amount of physical RAM installed.

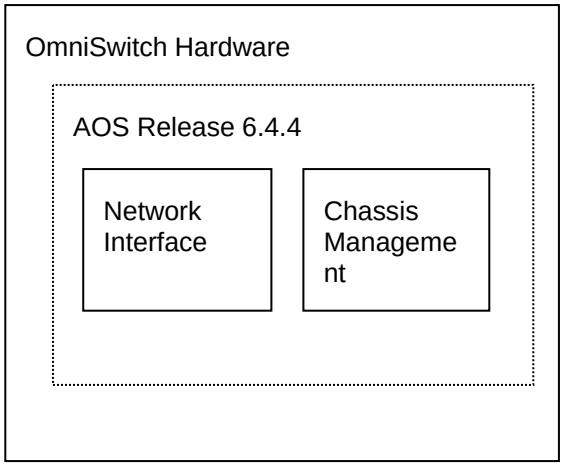


Figure 1: TOE Architecture

The OmniSwitch 6850E Series switches can also be linked together to form a single virtual chassis known as a stack. Likewise for the 6855 series and 6400 family of switches, stacking switches provides scalability by allowing quick and easy expansion of 10/100/1000 port density. Twenty four 10/100/1000 ports are added for each OS6850E-24 brought into the stack and forty-eight 10/100/1000 ports are added for each OS6850E-48. Up to eight switches can be stacked. OmniSwitch 6850E Series switches can be mixed and matched in any combination within the stack. This provides a virtual chassis with a 10/100/1000 capacity of up to 384 ports.

The term Chassis Managementis used to describe the logical management functionality of the TOEproviding services including:

- Console, USB, and Ethernet management port connections to the switch
- Software and configuration management, including the Command Line Interface (CLI)
- Power distribution
- Switch diagnostics
- Important availability features, including failover (when used in conjunction with another CMM), software rollback, temperature management, and power management
- The CMM also contains the switch fabric unit for the OS9000E Series switches. Data passing from one NI module to another passes through the CMM fabric. When two CMMs are installed, both fabrics are normally active.

For the OS6400, OS6850E, and OS6855, the Chassis Management functionality resides on the main processor PCB. The OS9000E series are chassis & blade based systems consisting of one or 2 Chassis Management Modules (CMM)s and 1-18 Network Interface (NI) modules. OS9700E-CMMs and OS9800E-CMMs use identical processor boards. However, OS9800E-CMMs use twice the number of network interface-related ASICs on the fabric board. This is because OS9800E switches support up to 16 network interface (NI) modules and OS9700 switches support up to 8 NI modules.

Network interface (NI) modules are categorized into GNI and XNI modules. Gigabit Ethernet Network Interface (GNI) modules provide 1000 Mbps (1 Gbps) connections. GNI modules can be used for backbone connections in networks where Gigabit Ethernet is used as the backbone media. XNI modules provide up to six 10000 Mbps (10 Gbps) connections per module and can be used in networks where 10-gigabit Ethernet is used as the backbone media.

## 1.4 Physical Boundaries

Figure 2 shows a depiction of the TOE and its operating environment. The operating environment may also include a syslog server which is not depicted in the figure below.

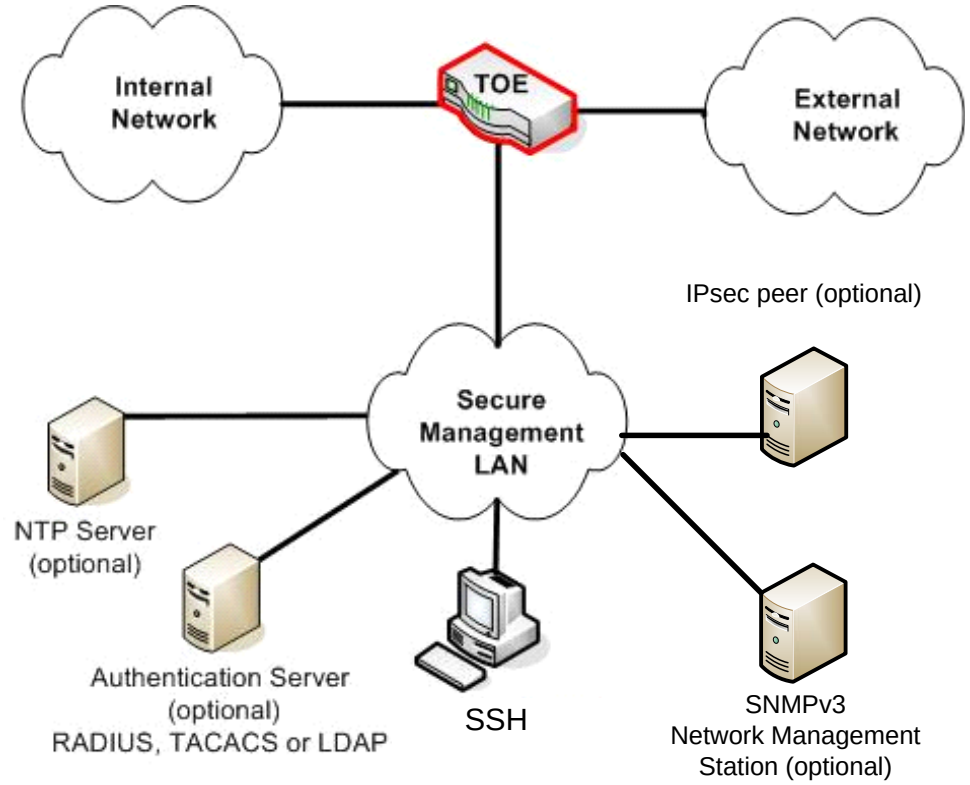


Figure 2: TOE Boundary

### 1.4.1 Hardware/OS Components

Table 1 below specifies the TOE hardware and software components that can be combined to form valid TOE configurations. In section 1.6.1, the acronym SFP is referring to Small Form Factor Pluggable transceivers. This should not be confused the CC acronym SFP used in Section 6 to refer to Security Function Policies.

| Hardware ID | Description |
|---|---|
| OmniSwitch 6400-24 | Gigabit Ethernet chassis in a 1U form factor with 20 RJ-45 ports individually configurable to 10/100/1000BaseT, four combo ports configurable to be 10/100/1000BaseT or 1000BaseX, and two dedicated 10G stacking ports. Combo ports support either copper or fiber can be used on a one for one basis. |
| OmniSwitch 6400-48 | Gigabit Ethernet chassis in a 1U form factor with 44 RJ-45 ports individually configurable to 10/100/1000BaseT, four combo ports configurable to be 10/100/1000BaseT or 1000BaseX, and two dedicated 10G stacking ports. Combo ports support either copper or fiber can be used on a one for one basis. |
| OmniSwitch 6400-U24 | Gigabit Ethernet chassis in a 1U form factor with 22 100/1000BaseX SFP ports, two combo ports configurable to be 10/100/1000BaseT or 100/1000BaseX, and two dedicated 10G stacking ports. Combo ports support either copper or fiber can be used on a one for one basis. This is an AC powered switch. |
| OmniSwitch 6400-U24D | Gigabit Ethernet chassis in a 1U form factor with 22 100/1000BaseX SFP ports, two combo ports configurable to be 10/100/1000BaseT or 100/1000BaseX, and two dedicated 10G stacking ports. Combo ports support either copper or fiber can be used on a one for one basis. This is a DC powered switch. |
| OmniSwitch 6400-P24 /P24H | Gigabit Ethernet chassis in a 1U form factor with 20 RJ-45 PoE (Power-over-Ethernet) ports individually configurable to 10/100/1000BaseT, four combo ports configurable to be 10/100/1000BaseT or 1000BaseX, and two dedicated 10G stacking ports. Combo ports support either copper or fiber can be used on a one for one basis.<br>The 6400-P24 supports 2 external 360W power supplies. The 6400-P24H supports 2 external 510W power supplies. |
| OmniSwitch 6400-P48 /P48H | Gigabit Ethernet chassis in a 1U form factor with 44 RJ-45 POE (Power-over-Ethernet) ports individually configurable to 10/100/1000BaseT, four combo ports configurable to be 10/100/1000BaseT or 1000BaseX, and two dedicated 10G stacking ports. Combo ports support either copper or fiber can be used on a one for one basis.<br>The 6400-P48 supports 2 external 360W power supplies. The 6400-P48H supports 2 external 510W power supplies. |
| OmniSwitch 6855-14 | Hardened Gigabit Ethernet fixed configuration fan-less switch in a 1U form factor designed to operate in harsh environments.<br>It has 12 RJ-45 connectors individually configurable to 10/100/1000BaseT, four of which are PoE (Power Over Ethernet) capable and two SFP ports which support various distances. |
| OmniSwitch 6855-U10 | Hardened Gigabit Ethernet fixed configuration fan-less switch in a 1U form factor designed to operate in harsh environments.<br>It has two RJ-45 connectors individually configurable to 10/100/1000BaseT, and eight SFP ports which support various distances. |
| OmniSwitch 6855-24 | Hardened Gigabit Ethernet fixed configuration switch in a 1U form factor designed to operate in harsh environments.<br>It has 20 RJ-45 connectors individually configurable to 10/100/1000BaseT, four of which provide PoE (Power Over Ethernet) and four combo ports. On the combo ports, either copper or fiber can be used on a one-for-one basis. |
| OmniSwitch 6855-U24 | Hardened Gigabit Ethernet fixed configuration switch in a 1U form factor designed to operate in harsh environments.<br>It has 22 SFP ports which support various distances, and two combo ports. On the combo ports, either RJ-45 connectors individually configurable to 10/100/1000BaseT, or fiber SFP can be used on a one-for-one basis. |

| | |
|---|---|
| OmniSwitch 6850E–24 | Gigabit Ethernet chassis in a 1U form factor with 20 RJ-45 ports individually configurable to 10/100/1000 BaseT, 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, and two dedicated stacking ports. |
| OmniSwitch 6850E–24X | Gigabit Ethernet chassis in a 1U form factor with 20 RJ-45 ports individually configurable to 10/100/1000 BaseT, 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, two 10 Gigabit ports, and two dedicated stacking ports. |
| OmniSwitch 6850E–48 | Gigabit Ethernet chassis in a 1U form factor with 44 RJ-45 ports individually configurable to 10/100/1000 BaseT, 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, and two dedicated stacking ports. |
| OmniSwitch 6850E–48X | Gigabit Ethernet chassis in a 1U form factor with 48 RJ-45 ports individually configurable to 10/100/1000 BaseT, two 10 Gigabit ports, and two dedicated stacking ports. |
| OmniSwitch 6850E–U24X | Gigabit Ethernet chassis in a 1U form factor with 22 1000 Base-X SFP ports, 2 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, two 10 Gigabit ports, and two dedicated stacking ports. |
| OmniSwitch 6850E–P24 | Gigabit Ethernet chassis in a 1U form factor with 20 RJ-45 PoE (Power Over Ethernet) ports individually configurable to 10/100/1000 BaseT, 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, and two dedicated stacking ports. |
| OmniSwitch 6850E–P24X | Gigabit Ethernet chassis in a 1U form factor with 20 RJ-45 PoE (Power Over Ethernet) ports individually configurable to 10/100/1000 BaseT, 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, two 10 Gigabit ports, and two dedicated stacking ports. |
| OmniSwitch 6850E–P48 | Gigabit Ethernet chassis in a 1U form factor with 44 RJ-45 PoE (Power Over Ethernet) ports individually configurable to 10/100/1000 BaseT, 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, and two dedicated stacking ports. |
| OmniSwitch 6850E–P48X | Gigabit Ethernet chassis in a 1U form factor with 48 RJ-45 PoE (Power Over Ethernet) ports individually configurable to 10/100/1000 BaseT, two 10 Gigabit ports, and two dedicated stacking ports. |
| OmniSwitch 6850E–24L | Gigabit Ethernet chassis in a 1U form factor with 20 RJ-45 ports individually configurable to 10/100 BaseT, 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, and two dedicated stacking ports. |
| OmniSwitch 6850E–48L | Gigabit Ethernet chassis in a 1U form factor with 44 RJ-45 ports individually configurable to 10/100 BaseT, 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, and two dedicated stacking ports. |
| OmniSwitch 6850E–P24L | Gigabit Ethernet chassis in a 1U form factor with 20 RJ-45 PoE (Power Over Ethernet) ports individually configurable to 10/100 BaseT, 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, and two dedicated stacking ports. |
| OmniSwitch 6850E–P48L | Gigabit Ethernet chassis in a 1U form factor with 44 RJ-45 PoE (Power Over Ethernet) ports individually configurable to 10/100 BaseT, 4 combo ports configurable to be 10/100/1000 BaseT or 1000 BaseX, and two dedicated stacking ports. |
| OmniSwitch 9800E chassis | A chassis with two slots for CMMs and 16 slots for NI modules. |
| OmniSwitch 9700E chassis | A chassis with two slots for CMMs and 8slots for NI modules. |
| **OS ID** | **Description** |
| AOS version 6.4.4 | The single purpose operating system that provides TOE Management and enforcement functions. It is provided on all platforms. The complete software version identification is AOS Release 6.4.4.342.R01 can be confirmed on the TOE using the **show system** command. |

Table 1: TOE Physical Components

The OS9000E series require at least one Chassis Management Module (CMM) and at least one Network Interface (NI) modules. Table 2 below specifies the TOE hardware CMM and NI modules for the 9000E series that can be used to form valid TOE configurations:

| Hardware ID | Description |
|---|---|
| OS9800E-CMM | 9800E series CMM |
| OS9700E-CMM | 9700E series CMM |
| OS9-GNI-C24E | Provides 24 auto-sensing twisted-pair ports, individually configurable as 10BaseT, 100BaseTX, or 1000BaseT |
| OS9-GNI-U24E | Provides 24 SFP connectors. |
| OS9-XNI-U2E | Provides two XFP connectors. |

Table 2: TOE Physical Components – 9000E Series modules

### 1.4.2 Operational Environment

This section describes requirements on the environment in which the TOE is operated. The intended TOE environment is a secure data center that protects the TOE from unauthorized physical access. Only authorized administrators are to have access to connect to the serial console, or gain physical access to the hardware storing log data. Appropriate administrator security policy and security procedure guidance must be in place to govern operational management of the TOE within its operational environment.

- The Operational Environment must include a SSHv2 client
- If the TOE is configured to use RADIUS, TACACS+, or LDAP authentication, the TOE is dependent upon a RADIUS, TACACS+, or LDAP authentication server in the TOE operational environment.
- If the TOE is configured for use of LDAP with SSL, the TOE is dependent upon a SSLv2, SSLv3 or SSL v3.1 / TLS 1.0 LDAP capable server.
- If the TOE is configured to perform IEEE 802.1X authentication, then the TOE is dependent upon an IEEE 802.1X client to be on the physical device attached to the LAN port in the TOE operating environment. This client is built into most standard current operating systems. In addition, if 802.1X is enabled, the TOE is dependent upon a RADIUS authentication serer in the TOE operational environment.
- If time is being synchronized to an external time source, a Network Time Protocol (NTP) server is required in the operational environment.
- If the TOE is configured to use SNMP, only SNMPv3 may be used with the “snmp privacy all” setting; in this case, an SNMP/SNMPv3 Network Management Station is required in the operational environment.
- If the TOE is configured to send switch logging output files (syslog files) to a remote IP address, a syslog server is required in the operational environment.
- If the TOE is configured to use IPsec, at least one IPsec peer is required in the operational environment.

A serial console connected to the appliance must at a minimum be available for installation and initial configuration. The serial console is optional once the installation and configuration is completed.

## 1.5 Logical Boundaries

This section contains the product features and denotes which are in the TOE.

### 1.5.1 Audit

The TOE generates audit records. The audit records are displayed on the CLI console as they are generated in a scrolling format.

The TOE writes audit logs to a text file stored in the systems flash memory for permanent storage. These audit log entries are tagged with the AOS Application that created them. The TOE also provides the ability to send switch logging information to an external syslog server.

The TOE provides the authorized administrator with the ability to increase the size of the log files from the default value of 128k to the capacity of the flash drive. Once the files are full the oldest entries are overwritten.

### 1.5.2 Identification and Authentication

There are two types of authentication performed by the TOE: Authorized Administrator Authentication and End-user Authentication (the term end-user refers to the device on the network.)

Administrator authentication can be performed locally on the TOE or the TOE can rely upon an external authentication server in the operational environment to authenticate an administrative-user (the term administrative-user refers to operators authorized to perform administrative functions). The external authentication servers supported by the TOE for administrator authentication are RADIUS, and TACACS+; an external LDAP server provides information useful in access control, but does not perform authentication.

End-user (device) authentication is used to mediate network information flows. The end-user authentication is performed by verifying the credentials of either the device or the device operator. The TOE supports three types of end-user authentication: MAC authentication, web-based authentication (Captive Portal), and IEEE 802.1X. These authentication methods require an external authentication server in the operational environment.

The TOE provides administrator configurable password settings to enforce local password complexity when a password is created or modified. The TOE also provides the ability to lockout administrative-users after an administrator configurable number of consecutive unsuccessful local authentication attempts.

#### *1.5.2.1 Authorized Administrator Authentication*

Administrator authentication (also known as Authenticated Switch Access (ASA)) can be performed locally on the TOE or the TOE can rely upon an external authentication server in the operational environment to authenticate the administrative-user. The external authentication servers supported by the TOE for administrator authentication are LDAP, RADIUS, and TACACS+.

Whether through serial console, SSH or SNMPv3 the TOE requires the administrator to identify and authenticate to the TOE prior to accessing any of the management functionality.

The TOE itself can provide administrator authentication and store the credentials of administrators authenticated locally by the TOE. It is possible, though not required, to configure a LDAP / RADIUS / TACACS+ authentication server in the TOE operating environment to store the credentials and perform the identification and authentication. There is a single role of authorized administrator for the TOE.

Finally, every SNMPv3 packet is authenticated using HMAC-MD5 or HMAC-SHA as described in Section 7.2.4.

#### *1.5.2.2 MAC Authentication*

The TOE provides MAC authentication which verifies the identity of the end-user (device) by sending the request to a RADIUS server for verifying the MAC address.

#### *1.5.2.3 Captive Portal Authentication*

The TOE provides web-based authentication which allows end-users to authenticate by providing their credentials through their web browser.

#### *1.5.2.4 IEEE 802.1X*

Physical devices attached to a LAN port on the TOE are authenticated by the TOE through IEEE 802.1X using the Extensible Authentication Protocol (EAP). This feature provides port-based Network Access Control for external devices.

There are three components for 802.1X:

- The Supplicant. This is the device residing in the TOE operating environment that supports the 802.1x protocol and is connected to the TOE. The device may be connected directly to the switch or via a point-to-point LAN segment. Typically the supplicant is a PC or laptop. A client is installed on the supplicant to support 802.1X authentication.
- The Authenticator Port Access Entity (PAE). This entity requires authentication from the supplicant. The authenticator is connected to the supplicant directly or via a point-to-point LAN segment. The TOE acts as the authenticator.
- The Authentication Server. This component resides in the TOE operating environment and provides the authentication service and verifies credentials (username, password, challenge, etc.) of the supplicant. The credentials to be verified can be the credentials of the device or a human operator. Note only RADIUS servers are supported for 802.1X authentication.

Figure 3 shows a depiction of IEEE 802.1X device authentication provided by the TOE.

NOTE: 802.1X is the recommended solution to provide the highest level of security for end-user authentication.

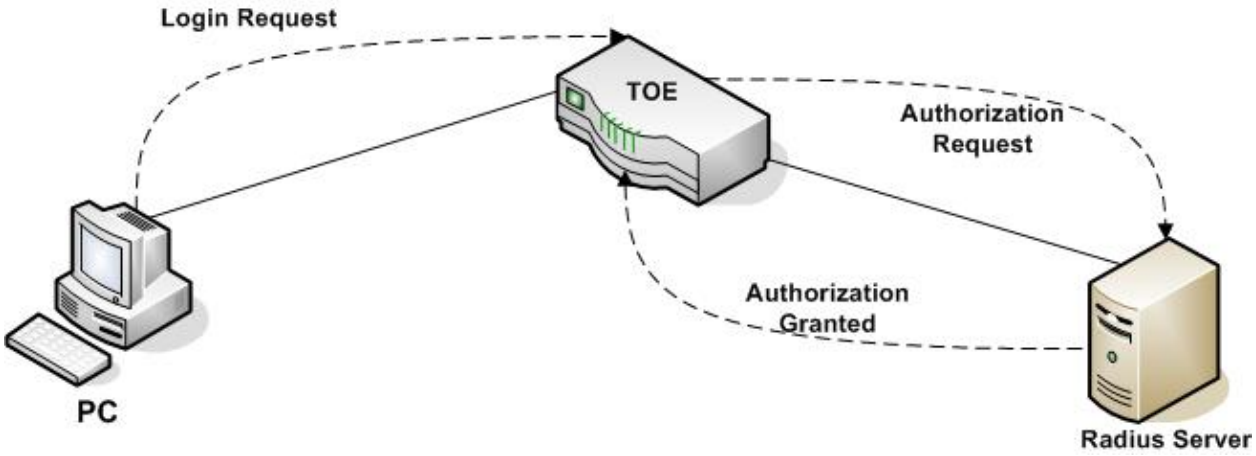


Figure 3: IEEE 802.1X device authentication

### 1.5.3 Management of the TOE

The TOE provides the CLI for the TOE's security management functionality. The TOE also provides SNMPv3 management interfaces as well as a Flash file system for storing configuration files/directories. Files can be transferred to the Flash file system via SFTP.

The TOE provides the administrator the ability to create, modify & delete policies that meditate traffic flow as implemented by the Traffic Filter SFP or VLAN SFP.

The TOE provides the administrator the ability to manage all other aspects of the TOE; for example, configuring local administrator accounts and viewing or configuring the audit trail.

### 1.5.4 Traffic Mediation and Filtering

The TOE can mediate traffic using one of the following 2 methods:

| | |
|---|---|
| VLANs and 802.1Q | The TOE will note the VLAN ID of the packet when it's received on the port. The packet is then bridged to other ports that are assigned to the same VLAN ID but not other ports.<br><br>For 802.1Q deployments, the TOE 'tags' packets from a given source with a Logical Network identification (VLAN Tag) indicating which VLAN its allowed to access. If the egress port of the TOE is configured for 802.1Q for that VLAN, the TOE will re-insert the 802.1Q tag. The TOE then forwards the frame. This method also allows the TOE to bridge traffic for multiple VLANs over one physical port connection. The TOE will always enforce VLAN separation by only allowing packets onto the VLAN that matches the VLAN Tag. VLAN traffic will not be forwarded to interfaces not in that VLAN.<br><br>Once traffic is allocated to a logical network (VLAN) the TOE will mediate the traffic to ensure that traffic in one logical network is not available to traffic in another logical network without further mediation (IP forwarding). |
| Traffic Filter | Once traffic has been allocated to a logical network (VLAN), the TOE can filter packets based on global settings and Access Control Lists to allow that traffic to leave its logical network and access another. Packet flows arriving at a network interface of the TOE are checked to ensure that they conform to the configured traffic filter policy. |

User Network profiles simplify the network infrastructure security configuration by dynamically controlling authentication of operators and devices while reducing administrative overhead because less human intervention is needed for common tasks such as additions, moves and changes. User Network profiles enforce operator and device access compliance through access control for user groups at the switch port.

#### *1.5.4.1 VLANs*

For static (non-mobile) ports, when a packet is received, the TOE inserts the port's VLAN ID into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID. See Figure 4 for an example.

The TOE also supports mobile ports which provide a dynamic VLAN identification. It allows the TOE to receive and process frames tagged with VLAN identification (802.1Q) in the packet header. In this deployment, the TOE 'tags' packets from a given source with a Logical Network identification (VLAN Tag) indicating which VLAN its allowed to access. The TOE then forwards the frame. This method also allows the TOE to bridge traffic for multiple VLANs over one physical port connection. The TOE will enforce VLAN separation by only allowing packets onto the VLAN that matches the VLAN Tag. VLAN traffic will not be forwarded to interfaces not in that VLAN.

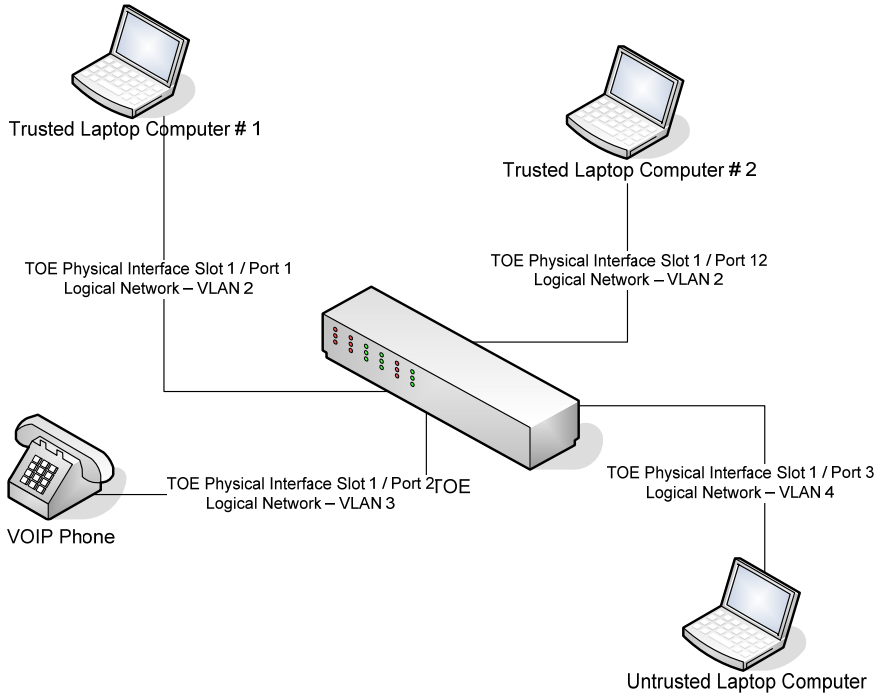


Figure 4: Static VLAN port configuration

### *1.5.4.2 Forwarding (Routing)*

If a device needs to communicate with another device that belongs to a different VLAN, the TOE mediates the flow of information between the VLANs.

As depicted in the figure below, Layer-3 routing is necessary to transmit traffic between the VLANs. A VLAN is available for routing if an IP interface has been configured for forwarding on that VLAN. Therefore, workstations connected to ports on VLAN 1 can communicate with ports on VLAN 3.

If a VLAN does not have a router interface configured, the ports associated with the VLAN are isolated from other VLANs.

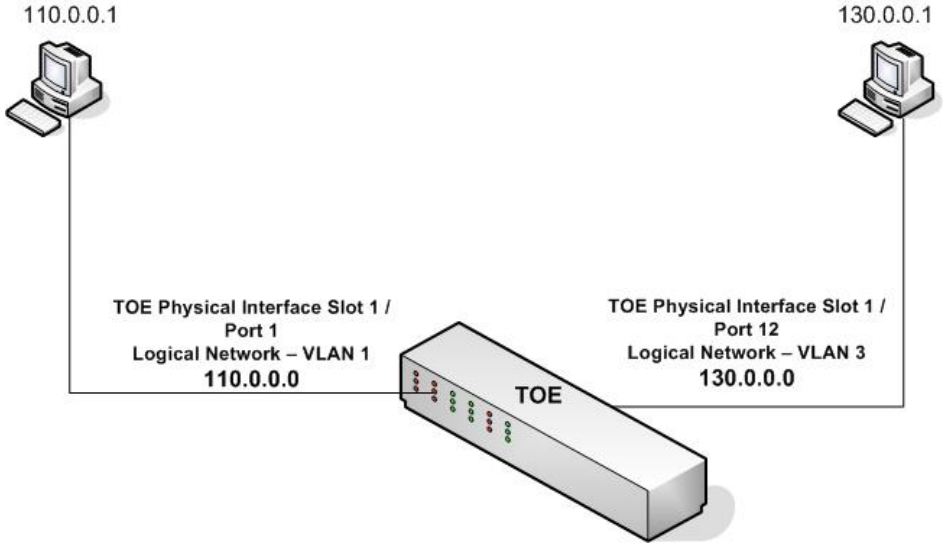


Figure 5: IP Forwarding

#### *1.5.4.3 Traffic Filtering*

Traffic Filtering is implemented using Access Control Lists to moderate traffic flow between networks. When traffic arrives on the switch, the switch checks its policy database to attempt to match Layer-2 (bridging) or Layer-3 / 4 information (routing) in the packet header to a filtering policy rule. If a match is found, it applies the permit or deny operation assigned to the rule. The default is to allow the traffic. This default can be changed by an administrator.

The TOE can filter traffic at Layer-2 based on MAC address or MAC group; source VLAN; or physical slot/port or port group. The TOE can filter traffic at Layer-3 based on source IP address or source network group; destination IP address or destination network group; IP protocol; ICMP code or type; source TCP/UDP port; or destination TCP/UDP port or service or service group. The TOE can perform limited filtering of IPv6 traffic, and can filter multicast traffic via the Internet Group Management Protocol (IGMP). Figure 6 depicts examples of traffic filtering.

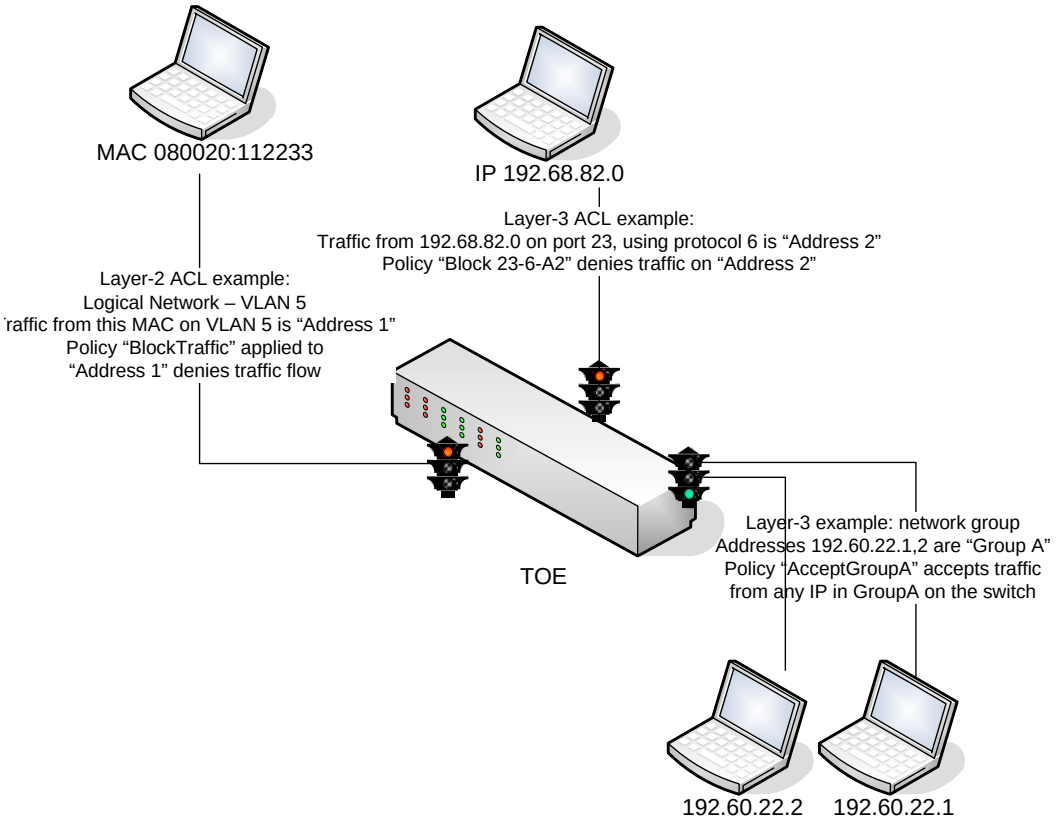


Figure 6: Traffic Filtering

## 1.5.5 Protection of the TSF

The switches protect themselves by requiring administrators to identify and authenticate themselves prior to performing any actions and by defining the access allowed by each administrator.

The TOE is not intended for use as a general purpose computer and only executes the services needed to perform its intended function

The TOE provides secure access for the administrator to manage the TOE via SNMPv3 or SSH v2 (including SFTP). The TOE implements SSLv2, SSLv3 and SSL v3.1 / TLS 1.0:throughout this document, any reference to “SSL” or “TLS” refers to any of these SSL or TLS versions. TLS 1.0 is an alternative name for SSL v3.1, which is backward compatible with SSLv2 and SSLv3.

#### *1.5.5.1 IPsec*

IPsec is a suite of protocols for securing Internet Protocol (IP) traffic. On IPv6, the TOE provides IPsec to secure the exchange of route information with external routers. The TOE provides IPsec encryption/decryption as is specified in the IPv6 version of OSPFv3.

The IPsec implementation supports only manual IPsec key management to distribute the cryptographic keys. (Internet Key Exchange (IKE) key management is not provided.)

IPsec is a purchase option. The 6400 Series does not support IPsec. The 6855 Series, 6850E Series and 9000 Series support IPsec with the following IPsec options:

1. ESP confidentiality and integrity
2. ESP confidentiality and AH authentication

### 1.5.6 Non-Security Relevant TOE Features

The following table identifies other AOS features that are not security relevant and their usage does not impact the overall security of the product.

| Feature | Description |
|---|---|
| LDAP Policy Server | LDAP Policy Server features are used to manage LDAP Policies. LDAP policies are Quality of Service (QoS) policies that are created via the PolicyView application and stored on an external LDAP server. The Policy Manager in the switch downloads these policies and keeps track of them. These policies cannot be modified directly on the switch. Since policies may only be modified via their originating source, LDAP policies must be modified through PolicyView and downloaded again to the switch. |
| Load balancing | Server Load Balancing (SLB) allows clients to send requests to servers logically grouped together in clusters. Each cluster logically aggregates a set of servers running identical applications with access to the same content (e.g., web servers). SLB uses a Virtual IP (VIP) address to treat a group of physical servers, each with a unique IP address, as one large virtual server. The switch will process requests by clients addressed to the VIP of the SLB cluster and send them to the physical servers. This process is totally transparent to the client. |
| DVMRP / PIM | IP Multicast Routing Protocols |
| AMAP (Mapping Adjacency Protocol) | The switch is able to discover and advertise adjacent switch information using one of its Interswitch Protocols (AIP) called the Mapping Adjacency Protocol (AMAP). Below you will see all the AMAP supported switches adjacent to this switch. |
| Spanning Tree (STP) | The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. Based on the IEEE 802.1D standard, the Alcatel STP implementation distributes the Spanning Tree load between the primary management module and the network interface modules. In the case of a stack of switches, the STP load is distributed between the primary management switch and other switches in the stack |
| Link Aggregation | Link aggregation allows you to combine 2, 4, or 8 physical connections into large virtual connections known as link aggregation groups. You can create Virtual LANs (VLANs), configure Quality of Service (QoS) conditions, 802.1Q framing, and other networking features on link aggregation groups because the switch's software treats these virtual links just like physical links. |

Table 3: TOE functionality excluded from the TSF

### 1.5.7 Excluded TOE Features

The following features interfere with the TOE security functionality claims and must be disabled or not configured for use in the evaluated configuration.

1. Authenticated VLAN

   An authenticated VLAN grants end-users access to one or more VLANs after successful authentication at the switch port. Authenticated VLAN permissions are granted to end-users (not devices) leveraging external RADIUS, or LDAP directory servers

   This feature is superseded by Captive Portal and has been kept in the product for backwards compatibility reasons.

   a. Alcatel-Lucent-proprietary authentication client for VLAN-authentication
   b. Telnet authentication client for VLAN-authentication

2. IPX forwarding (routing)

   This feature has been kept in the product for backwards compatibility reasons.

3. Specifying an external RSA ACE/Server[2] to be used for authenticated switch access

   The TOE includes an ACE client version 4.1. An external ACE/Server can provide login information while operator authorization information is provided by the switch. Administrators are instructed to not use ACE/Server authentication in the evaluated configuration.

4. Port Mobility Rules

   Port mobility allows dynamic VLAN port assignment based on VLAN rules that are applied to port traffic.

   This feature is superseded by User network profiles and has been kept in the product for backwards compatibility reasons.

5. FTP access to the switch

   FTP traffic is not secured so the FTP service must be disabled for security reasons.

6. Telnet access to the switch

   Telnet traffic is not secured so the Telnet service must be disabled for security reasons.

7. Webview

   The Webview interface is not sufficiently documented for this evaluation; the WebView interface (also described as http in some Alcatel-Lucent documentation) must be disabled.

8. SNMPv1/v2/v3 access to the switch

   The TOE supports SNMPv1/v2/v3. SNMPv3 supports options to encrypt and authenticate traffic; without these provisions, administrative traffic is not secured. In the CC Evaluated Configuration, if SNMP is used, the TOE must be configured to use SNMPv3 encryption and authentication (snmp privacy all).

[2] The RSA ACE/Server is part of RSA Security's SecurID product suite.

## 1.6 Document Terminology

| Term | Definition |
|---|---|
| ACL | Access control List |
| Administrative-user | An administrative user of the TOE, authorized to control TOE settings, as opposed to end-users, associated with general network traffic |
| AOS | Alcatel Operating System for the switches |
| ASIC | Application-Specific Integrated Circuit |
| ASA | Authenticated Switch Access |
| Appletalk | AppleTalk protocol. Also captures Datagram Delivery Protocol (DDP) and AppleTalk ARP (AARP). |
| Application | In the context of AOS auditing there are several ‘applications’ that log records. These are identified by a number and abbreviation. |
| ASA | Authenticated Switch Access |
| Authenticated VLANs | Authenticated VLANs control operator access to network resources based on VLAN assignment and a operator log-in process; |
| BGP | Border Gateway Protocol |
| BOOTP | Bootstrap Protocol |
| CMM | Chassis Management Module  Physically a separate blade for 9000 series switches. Logically a separate piece of functionality built into the Management of the 6850E series |
| Decnet | DECNET Phase IV (6003) protocol. |
| DHCP | Dynamic Host Configuration Protocol |
| DSA | Digital Signature Algorithm |
| DSS | Digital Signature Standard |
| EAP | Extensible Authentication Protocol |
| End-user | Network traffic, non-administrative users of the TOE |
| GNI | Gigabit Ethernet Network Interface |
| GigE | Gigabit Ethernet |
| HMAC | Keyed-Hash Message Authentication Code |
| HTTPS | Hypertext Transfer Protocol Secure |
| IEEE 802.1X | IEEE 802.1X is an IEEE Standard for port-based Network Access Control |
| IGMP | Internet Group Management Protocol |
| IP | Internet Protocol |
| ip-e2 | IP Ethernet-II protocol. Also captures Address Resolution Protocol (ARP) |
| ip-snap | IP SNAP protocol |
| ipv6 | IPv6 protocol |
| IPX | Internet Protocol Exchange |
| LDAP | Lightweight Directory Access Protocol |
| MAC Address | Media Access Control Address, also known as the hardware or adaptor address. |
| NI | Network Interface Module.  Physically a separate blade for the 9000 series switches.  Logically a separate piece of functionality built into the Management of the 6850E series |
| OSPF | Open Shortest Path First is a dynamic routing protocol. |
| OS6400 | Alcatel-Lucent OmniSwitch, 6400 Series with AOS Release 6.4.4 |
| OS6850E | Alcatel-Lucent OmniSwitch 6850E Series with AOS Release 6.4.4 |
| OS6855 | Alcatel-Lucent Omniswitch 6855 Series with AOS Release 6.4.4 |
| OS9000E | Alcatel-Lucent OmniSwitches 9000E Series with AOS Release 6.4.4 |
| POE | Power over Ethernet |

| Term | Definition |
|---|---|
| Port Mobility | The ability for the Alcatel Switches to dynamically tag incoming traffic into a specific VLAN irrespective of the physical port the traffic enters |
| QoS | Quality of Service |
| RADIUS | Remote Authentication Dial In User Service |
| RIP | Routing information Protocol is a dynamic routing protocol. |
| SFP | Small Form Factor Pluggable transceiver (used in Section 1.4.1)<br>Or<br>Security Function Policies (used in Section 6) |
| SLB | Server Load Balancing |
| SNMP | Simple Network Management Protocol (inclusive of functionality from all supported versions of SNMP). SNMPv3 provides data confidentiality and integrity features. |
| SSH | Secure Shell |
| Stackable | 6850E series switches that can be connected with a special function cable that allows them to function as a virtual chassis using a central management point |
| TACACS+ | Terminal Access Controller Access Control System |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| VLAN, (Virtual LAN) / Logical Network | The term VLAN was specified by IEEE 802.1Q; it defines a method of differentiating traffic on a LAN by tagging the Ethernet frames. By extension, VLAN is used to mean the traffic separated by Ethernet frame tagging or similar mechanisms. In this ST Logical network and VLAN are used interchangeably |
| VoIP | Voice Over IP |
| WebView | The web based GUI to manage the TOE |
| XNI | 10-gigabit Ethernet Network Interface |

Table 4: Document Terminology

# 2 Conformance Claims

## 2.1 CC Conformance Claim

This ST was developed to Common Criteria (CC) for Information Technology Security Evaluation Part 1 – September 2006 Version 3.1, Revision 3 and CC for Information Technology Security Evaluation Parts 2 & 3 – September 2007 Version 3.1 Revision 3.

The ST claims to be:

CC Version 3.1 Revision 3 Part 2 extended

CC Version 3.1 Revision 3 Part 3 conformant

## 2.2 PP and Package Claims

The ST claims to be Evaluation Assurance Level 2 augmented with ALC_FLR.2.

The ST is not conformant to any Protection Profiles.

# 3 TOE Security Environment

The TOE is intended to be used in a physically secure environment

## 3.1 Assumptions

The assumptions are ordered into three groups relating to personnel operating the TOE, the physical environment around the TOE and the daily operation of the TOE.

### 3.1.1 Personnel Assumptions

| | |
|---|---|
| A.NOEVIL | The TOE administrator is not willfully negligent in the use of the TOE. |
| A.TRAIN | The TOE administrator is trained in the correct & secure usage of the TOE. |
| A.AUDREV | The TOE administrator will periodically review the audit logs on the TOE. |

### 3.1.2 Physical Environment Assumptions

| | |
|---|---|
| A.LOCATE | The TOE shall be located in a physically secure environment. |
| A.MGMTLAN | There will be a secure management network for the administrator to configure & manage the TOE. |

### 3.1.3 Operational Assumptions

| | |
|---|---|
| A.INTEROP | The TOE will be able to interact with other manufacturers' hardware attached to the network. |
| A.LOWEXP | The threat of malicious attacks aimed at exploiting the TOE is considered low. |

## 3.2 Threats

The TOE or Operating Environment addresses the threats identified in the following sections.

### 3.2.1 Threats Addressed by the TOE

The TOE addresses the threats discussed below.

The threat agents are authorized persons, unauthorized persons or external IT entities not authorized to use the TOE itself.

| | |
|---|---|
| T.NO_ADMINAUTH | An unauthorized person may attempt to bypass the security of the TOE to access and use functions provided by the TOE without authenticating. |
| T.NO_AUDIT | An administrative-user or end-user of the TOE may not be accountable for the actions they perform because their actions are not logged or an administrator does not review the audit records, thus allowing an attacker to escape detection. |
| T.NO_MEDIATE | An authorized entity may send impermissible information through the TOE, resulting in the exploitation of resources on the internal network. |
| T.NO_MGMT | The authorized administrator is not able to manage the secure functions of the TOE, causing the TOE to be configured in an insecure manner. |
| T.NO_TIME | The authorized administrator is not able to verify the audit trail because the audit records are not stamped with the correct time, thus allowing an attacker to escape detection. |
| T.RESIDUAL | An unauthorized person may gather residual information from a previous information flow. |
| T.SELPRO | An unauthorized person may read, modify, or destroy security critical TOE configuration data. |
| T.EAVESDROP | A malicious operator or process may observe or modify sensitive data transmitted between the TOE and a remote trusted IT entity. |

### 3.2.2 Threats Addressed by the Operating Environment

The operating environment addresses the threat discussed below. The threat is countered by procedural measures and /or administrative methods.

| | |
|---|---|
| TE.USAGE | The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons. |

# 4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

## 4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

| | |
|---|---|
| O.ACCESS | The authorized administrator is required to authenticate to the TOE before access to any of the TOE management functions is allowed. |
| O.AUDIT | The TOE will create a readable audit trail of security-related events, with accurate dates and times, for use by the administrator. |
| O.AUDREV | The TOE will provide a mechanism for the administrator to review the audit trail. |
| O.MEDIATE | The TOE will meditate all network traffic as defined by the policies created by the administrator and ensure that residual information from a previous information flow is not available. |
| O.SELPRO | The TOE will protect itself against attempts by unauthorized administrative-users to bypass, deactivate or tamper with TOE security functions. |
| O.TOE_MGMT | The TOE will provide interfaces to allow the administrator to configure the security functions of the TOE, including configuring policies to mediate traffic. |
| O.TRANSIT | The TSF shall protect TSF data when it is in transit between the TSF and a remote trusted IT entity. |
| O.TIME | The TOE will provide a time stamp for its own use. This time can be synchronized to an external time source via network time protocol (NTP). |

## 4.2 Security Objectives For The Environment

This section defines the security objectives that are to be addressed by the Operating Environment or by non-technical or procedural means.

### 4.2.1 Non-IT Security Objectives For The Environment

The non-IT security objectives listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures

| | |
|---|---|
| OE.ADMIN | The TOE administrators are trained in the correct and secure usage of the TOE. |
| OE.GUIDE | The TOE administrators must ensure that the TOE is delivered, installed, administered, and operated in a secure manner. |
| OE.PHYSEC | The TOE is located in a physically secure environment. |
| OE.MGMTLAN | The environment will provide a secure management network for the administrator to configure and manage the TOE |
| OE.NOEVIL | Authorized administrators are not willfully negligent in the use of the TOE. |

OE.AUDREV The authorized administrator will periodically review the audit trail on the TOE. Note that use of remote logging is in addition to local logging; the TOE always logs locally.

OE.LOWEXP There is a low expectation of malicious attacks against the TOE

OE.INTEROP The TOE will be able to interact with other manufacturers' network equipment attached to the network.

### 4.2.2 IT Security Objectives For The Environment

The following IT security objectives for the operating environment are to be addressed by technical means.

OE.IDAUTH If the TOE is configured to use external authentication, the TOE operating environment shall provide the ability to uniquely identify and authenticate end-users or administrative-users.

OE.SYSLOG If the TOE is configured to send switch logging output to a syslog server, the TOE operating environment shall provide permanent storage for the syslog files.

## 4.3 Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

| | T.NO_ADMINAUTH | T.NO_AUDIT | T.NO_MEDIATE | T.NO_MGMT | T.NO_TIME | T.RESIDUAL | T.SELPRO | T.EAVESDROP | TE.USAGE |
|---|---|---|---|---|---|---|---|---|---|
| O.ACCESS | X | | | | | | | | |
| O.AUDIT | | X | | | | | | | |
| O.AUDREV | | X | | | | | | | |
| O.MEDIATE | | | X | | | X | | | |
| O.SELPRO | | | | | | | X | | |
| O.TOE_MGMT | | | | X | | | | | |
| O.TRANSIT | | | | | | | | X | |
| O.TIME | | | | | X | | | | |
| OE.IDAUTH | X | | | | | | | | |
| OE.SYSLOG | | X | | | | | | | |
| OE.ADMIN | | | | | | | | | X |
| OE.GUIDE | | | | | | | | | X |

Table 5: Threats & Security Objectives Mappings

T.NO_ADMINAUTH An unauthorized person may attempt to bypass the security of the TOE to access and use functions provided by the TOE without authenticating.

O.ACCESS counters this threat by requiring the authorized administrator to authenticate to the TOE before allowing access to any TOE management functions.

| | |
|---|---|
| | OE.IDAUTH assists in countering this threat when the TOE is configured to use external authentication by requiring that the operating environment provide the ability to uniquely identify and authenticate administrative-users. |
| T.NO_AUDIT | An administrative-user of the TOE may not be accountable for the actions they perform because the actions are not logged or the audit records are not reviewed, thus allowing an attacker to escape detection. |
| | O.AUDIT counters this threat by ensuring that the TOE creates a readable audit trail of security-related events for use by the administrator. |
| | O.AUDREV counters this threat by providing a mechanism for the administrator to review the audit trail. This objective is met independent of the use of a syslog server. |
| | OE.SYSLOG assists in countering this threat when the TOE is configured to use a syslog server by providing permanent storage for switch logging output. |
| T.NO_MEDIATE | An authorized entity may send impermissible information through the TOE, resulting in the exploitation of resources on the internal network. |
| | O.MEDIATE counters this threat by requiring that all network traffic that passes through the network is mediated as defined by the policies created by the administrator. |
| T.NO_MGMT | The authorized administrator is not able to manage the secure functions of the TOE, causing the TOE to be configured in an insecure manner. |
| | O.TOE_MGMT counters this threat by providing interfaces to allow the administrator to configure the security functions of the TOE. |
| T.NO_TIME | The authorized administrator is not able to verify the audit trail because the audit records are not stamped with the correct time, thus allowing an attacker to escape detection. |
| | O.TIME counters this threat by requiring the TOE to provide a time stamp for its own use. |
| T.RESIDUAL | The unauthorized administrator may gather residual information from a previous information flow. |
| | O.MEDIATE counters this threat by ensuring that residual information from a previous information flow is not available. |
| T.SELPRO | An unauthorized person may read, modify, or destroy security critical TOE configuration data. |
| | O.SELPRO counters this threat by requiring that the TOE protect itself from attempts to bypass, deactivate, or tamper with the TOE security functions. |
| T.EAVESDROP | A malicious end-user or process may observe or modify end-user or TSF data transmitted between the TOE and a remote trusted IT entity. |

O.TRANSIT counters this threat by ensuring that the TOE protects TSF data when in transit between the TSF and a remote trusted IT entity.

TE.USAGE — The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

OE.ADMIN counters this threat by ensuring that the administrators are trained in the correct and secure usage of the TOE.

OE.GUIDE counters this threat by requiring that the TOE administrator ensure that the TOE is delivered, installed, administered, and operated in a secure manner.

## 4.4 Rationale For Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the environment cover that assumption.

| | A.NOEVIL | A.TRAIN | A.AUDREV | A.LOCATE | A.MGMTLAN | A.LOWEXP | A.INTEROP |
|---|---|---|---|---|---|---|---|
| OE.ADMIN | | X | | | | | |
| OE.PHYSEC | | | | x | | | |
| OE.MGMTLAN | | | | | x | | |
| OE.NOEVIL | x | | | | | | |
| OE.AUDREV | | | X | | | | |
| OE.LOWEXP | | | | | | X | |
| OE.INTEROP | | | | | | | X |

Table 6: Assumptions & Security Objectives Mappings for the Environment

A.NOEVIL — The TOE administrator is not willfully negligent in the use of the TOE.

OE.NOEVIL covers this assumption by ensuring that authorized administrators are non-hostile.

A.TRAIN — The TOE administrator is trained in the correct & secure usage of the TOE

OE.ADMIN covers this assumption by ensuring that the administrators are trained in the correct and secure usage of the TOE.

A.AUDREV — The TOE Administrator will periodically review the audit logs for the TOE

OE.AUDREV covers this assumption by requiring the authorized administrator to periodically review the audit trail on the TOE.

A.LOCATE — The TOE shall be used in a physically secure environment.

| | |
|---|---|
| | OE.PHYSEC covers this assumption by requiring that the TOE is located in a physically secure environment. |
| A.MGMTLAN | There will be a secure management network for the administrator to configure & manage the TOE. |
| | OE.MGMTLAN covers this assumption by requiring the environment to provide a secure management network for the administrator to configure and manage the TOE |
| A.INTEROP | The TOE will be able to interact with other manufacturers' hardware attached to the network. |
| | OE.INTEROP covers this assumption by requiring that the TOE is able to interact with other network equipment attached to the network. |
| A.LOWEXP | The threat of malicious attacks aimed at exploiting the TOE is considered low. |
| | OE.LOWEXP covers this assumption by requiring that there is a low expectation of malicious attacks against the TOE. |

# 5 Extended Components Definition

This section defines the newly defined components (also known as extended components) used to define the security requirements for this ST. The extended components defined in this section are members of existing CC Part 2 families and are based on the existing CC Part 2 SFRs.

## 5.1.1 FIA Identification and Authentication

The FIA class is extended to include four additional components.

The FIA class addresses the requirements to verify a claimed operator identity. The extended components defined in this section require the TOE to ensure that either the Operating environment or the TOE verifies claimed operator identities.

### *5.1.1.1 FIA_UAU_TRD.1 Timing of authentication with a third party*

FIA_UAU_TRD.1 is an extension to the FIA_UAU family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the authentication to be performed by the TOE or Operating environment, but required by the TOE. This extended SFR is based on CC Part 2 FIA_UAU.1.

Management: FIA_UAU_TRD.1

The following actions could be considered for the management functions in FIA:

- If authentication is by the TOE, management of the authentication data by an administrator
- If authentication is by the TOE, management of the authentication data by the associated administrative-user
- Managing the list of actions that can be taken before the administrative-user is authenticated.

Audit: FIA_UAU_TRD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism;
- Basic: All use of the authentication mechanism;
- Detailed: All TSF mediated actions performed before authentication of the administrative-user.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification or

FIA_UID_TRD.1 Time of identification with a third party or

FIA_UAU_SRV.1 Authentication via an external authentication server

FIA_UAU_TRD.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the administrative-user to be performed before the administrative-user is authenticated by the [selection: *Operating environment, TOE or the Operating environment as configured by the administrator*].

FIA_UAU_TRD.1.2 The TSF shall require each administrative-user to be successfully authenticated by the [selection: *Operating environment, TOE or the Operating environment as configured by the administrator*] before allowing any other TSF-mediated actions on behalf of that administrative-user.

### *5.1.1.2 FIA_UID_TRD.1 Timing of identification with a third party*

FIA_UID_TRD.1 is an extension to the FIA_UID family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the identification to be performed by the TOE or Operating environment, but required by the TOE. This extended SFR is based on CC Part 2 FIA_UID.1.

Management: FIA_UID_TRD.1

The following actions could be considered for the management functions in FIA:

- If identification is by the TOE, management of the administrative-user identities;
- If an authorized administrator can change the actions allowed before identification, the managing of the action lists.

Audit: FIA_UID_TRD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the administrative-user identification mechanism, including the administrative-user identity provided;
- Basic: All use of the administrative-user identification mechanism, including the user identity provided.

Hierarchical to: No other components.

Dependencies: None

FIA_UID_TRD.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the administrative-user to be performed before the administrative-user is identified by the [selection: *Operating environment, TOE or the Operating environment as configured by the administrator*].

FIA_UID_TRD.1.2 The TSF shall require each administrative-user to be successfully identified by the [selection: *Operating environment, TOE or the Operating environment as configured by the administrator*] before allowing any other TSF-mediated actions on behalf of that administrative-user.

#### *5.1.1.3 FIA_UAU_SRV.1 Authentication via an external authentication server*

FIA_UAU_SRV.1 is an extension to the FIA_UAU family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the authentication to be performed by an authentication server which is either part of the TOE or in the Operating environment. This extended SFR is based on CC Part 2 FIA_UAU.1.

Management: FIA_UAU_SRV.1

The following actions could be considered for the management functions in FIA:

- If authentication is by the TOE, management of the authentication data by an administrator
- If authentication is by the TOE, management of the authentication data by the associated administrative-user
- Configuration of the authentication server(s) used to authenticate administrative-users.

Audit: FIA_UAU_SRV.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism, including the administrative-user identity provided, if applicable;
- Basic: All use of the authentication mechanism, including the administrative-user identity provided, if applicable.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification or

FIA_UID_TRD.1 Timing of identification or

FIA_UID_SRV.1 Identification via an external authentication server.

FIA_UAU_SRV.1.1 When invoked by the TSF, the [assignment: list of authentication servers] in the [selection: *TOE*, *Operating environment*] shall determine if the administrative-user has provided valid authentication data and pass the results of that determination back to the TOE.

#### *5.1.1.4 FIA_UID_SRV.1 Identification via an external authentication server*

FIA_UID_SRV.1 is an extension to the FIA_UID family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the identification to be performed by an authentication server which is either part of the TOE or in the Operating environment. This extended SFR is based on CC Part 2 FIA_UID.1.

Management: FIA_UID_SRV.1

The following actions could be considered for the management functions in FIA:

- If the authentication server is in the TOE, management of the administrative-user identities;
- Configuration of the authentication server(s) used to identify administrative-users.

Audit: FIA_UID_SRV.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the administrative-user identification mechanism, including the administrative-user identity provided if applicable;
- Basic: All use of the administrative-user identification mechanism, including the administrative-user identity provided if applicable.

Hierarchical to: No other components.

Dependencies: None

FIA_UID_SRV.1.1 When invoked by the TSF, the [assignment: list of authentication servers] in the [selection: *TOE*, *Operating environment*] shall determine if the administrative-user has provided valid identification data and pass the results of that determination back to the TOE.

### 5.1.2 FTP Trusted path/channels

The FTP class is extended to include one additional component.

The FTP class provides requirements for a trusted communication path between administrative-users and the TSF and between the TSF and another trusted IT product. The extended components defined in this section do not require the TOE initiate communication for a list of functions.

#### *5.1.2.1 FTP_ITC_PDR.1 Inter-TSF trusted channel: Use of Channel*

FTP_ITC_PDR.1 is an extension to the FIA_ITC family. This extended requirement is necessary since a CC Part 2 SFR does not exist that does not require the TOE to initiate communication for some of the functions requiring a trusted channel.

This extended SFR is based on CC Part 2 FTP_ITC.1 and applies CCEVS PD-0108.

Management: FTP_ITC_PDR.1

The following actions could be considered for the management functions in FMT:

- Configuration of the actions that require a trusted channel, if supported.

Audit: FTP_ITC_PDR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Failure of the trusted channel functions.

- Minimal: Identification of the initiator and target of failed trusted channel functions.
- Basic: All attempted uses of the trusted channel functions.
- Basic: Identification of the initiator and target of all trusted channel functions.

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC_PDR.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_PDR.1.2 The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC_PDR.1.3 The TSF shall use a trusted channel for the following functions [assignment: list of functions for which a trusted channel is required].

# 6 IT Security Requirements

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

## 6.1 Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations.

**Assignment:** **indicated with bold text**

Selection: indicated with underlined text

***Refinement:*** ***indicated with bold text and italics for additions and bold-italic ~~strike-through~~ for deletions***

Iteration: indicated with typical CC requirement naming followed by an increasing number inside parenthesis following the requirements short name. Example: FCS_COP.1 (1).

## 6.2 TOE Security Functional Requirements

The TOE SFRs defined in this section are taken from CC Version 3.1 Part 2 or the extended components defined in Section 5.

| TOE Security Functional Requirements | |
|---|---|
| **Audit** | |
| FAU_GEN.1 | Audit Data Generation |
| FAU_SAR.1 | Audit Data Review |
| FAU_STG.1 | Protected Audit Trail Storage |
| **Cryptography** | |
| FCS_CKM.1 (1) | Cryptographic Key Generation (SSL Asymmetric Keys) |
| FCS_CKM.1 (2) | Cryptographic Key Generation (SSL Symmetric Keys) |
| FCS_CKM.1 (3) | Cryptographic Key Generation (SNMPv3 Keys) |
| FCS_CKM.1 (4) | Cryptographic Key Generation (SSH DSA Asymmetric Key Pair) |
| FCS_CKM.1 (5) | Cryptographic Key Generation (SSH Symmetric Key Derivation) |
| FCS_CKM.2 (1) | Cryptographic Key Distribution (SSL - RSA Public Keys) |
| FCS_CKM.2 (2) | Cryptographic Key Distribution (SSL – DH Symmetric Key Agreement) |
| FCS_CKM.2 (3) | Cryptographic Key Distribution (SSH – DH Symmetric Key Agreement) |
| FCS_CKM.2 (4) | Cryptographic Key Distribution (SSH - DSA Public Keys) |
| FCS_CKM.4 | Cryptographic Key Destruction |
| FCS_COP.1 (1) | Cryptographic Operation – SSL Session |
| FCS_COP.1 (2) | Cryptographic Operation – SSL Signing |
| FCS_COP.1 (3) | Cryptographic Operation – Hashing |
| FCS_COP.1 (4) | Cryptographic Operation – SSH Session |

| | |
|---|---|
| FCS_COP.1 (5) | Cryptographic Operation – IPsec encryption services |
| FCS_COP.1 (6) | Cryptographic Operation – SNMPv3 encryption services |
| **Identification & Authentication** | |
| FIA_ATD.1 | Administrative-User Attribute Definition |
| FIA_AFL.1(1) | Authentication Failure Handling – User |
| FIA_AFL.1(2) | Authentication Failure Handling – Session |
| FIA_SOS.1 | Verification of Secrets |
| FIA_UAU_TRD.1 | Timing of Authentication with a third party |
| FIA_UID_TRD.1 | Timing Of Identification with a third party |
| FIA_UAU.5 | Multiple Authentication Mechanisms |
| **Information Flow Control** | |
| FDP_IFC.1 (1) | Subset information flow Control (Traffic Filter) |
| FDP_IFF.1 (1) | Simple Security Attributes (Traffic Filter) |
| FDP_IFC.1 (2) | Subset information flow Control (VLAN) |
| FDP_IFF.1 (2) | Simple Security Attributes (VLAN) |
| FDP_RIP.1 | Subset Residual Information Protection |
| **Security Management** | |
| FMT_MSA.1 | Management of Security Attributes |
| FMT_MSA.3 | Static attribute initialization |
| FMT_MOF.1 | Management of the TOE |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Security Roles |
| **Protection of the TSF** | |
| FPT_STM.1 | Reliable Time stamps |
| **TOE Access** | |
| FTA_SSL.3(1) | TSF-initiated termination – login attempt session |
| FTA_SSL.3(2) | TSF-initiated termination – user session |
| **Trusted path/channels** | |
| FTP_ITC.1 | Inter-TSF trusted channel |
| FTP_ITC_PDR.1 | Inter-TSF trusted channel: Use of Channel |

Table 7: Functional Requirements

## 6.2.1 Security Audit (FAU)

#### *6.2.1.1 FAU_GEN.1 Audit Data Generation*

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

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

b) All auditable events for the not specified level of audit; and

c) **See Table 8.**

| SFR | Action | Details |
|---|---|---|
| FDP_IFF.1 (1) | All decisions on requests for information flow made by the Traffic Filter SFP | None |
| FIA_UAU_TRD.1 | All use of the Administrator Authentication Mechanisms | None |
| FIA_UID_TRD.1 | All use of the Administrator Identification Mechanisms | None |
| FIA_UAU.5 | The final authentication decision. | Administrative-user identities provided to the TOE |
| FMT_MOF.1 | All Modifications to the behavior of the TSF | None |
| FMT_MSA.1 | All offered & rejected values for a security attribute | None |
| FMT_MSA.3 | Modifications to the default permissive rules | None |
| FMT_SMF.1 | Use of the Management functions | None |
| FMT_SMR.1 | Modifications to the group of uses that are part of a role | None |
| FPT_STM.1 | Changes to the time | None |

Table 8: Audit Generation details

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **see Table 8**.

#### *6.2.1.2 FAU_SAR.1 Audit review*

FAU_SAR.1.1 The TSF shall provide **the administrator** with the capability to read **all recorded information** from the audit records.

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

#### *6.2.1.3 FAU_STG.1 Protected audit trail storage*

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

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail**.**

### 6.2.2 Cryptographic Operations (FCS)

The cryptography defined in this section has not been FIPS certified nor has it been analyzed or tested to confirm to cryptographic standards during the evaluation. All cryptography has only been asserted as tested by the vendor.

#### *6.2.2.1 FCS_CKM.1 (1) Cryptographic key generation (SSL Asymmetric Keys)*

FCS_CKM.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithms **RSA ANSI X9.31** and specified cryptographic key sizes **1024 bit** that meet the following: **RSA ANSI X9.31.**

#### *6.2.2.2 FCS_CKM.1 (2) Cryptographic key generation (SSL Symmetric Keys)*

FCS_CKM.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **as defined in the SSL v3 standard** and specified cryptographic key sizes **128 bit (RC4), 168 bit (TDES), 128 bit (AES), 256 bit (AES)** that meet the following: **SSL v3 standard[3] section 6.2.**

*Application Note This requirement addresses the distribution aspect of SSL session key agreement.*

#### *6.2.2.3 FCS_CKM.1 (3) Cryptographic Key Generation (SNMPv3 Keys)*

FCS_CKM.1(3) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **USM for SNMPv3** and specified cryptographic key sizes **56 bits** that meet the following: **generation of DES authentication and privacy keys as defined in USM for SNMPv3 RFC3414**.

#### *6.2.2.4 FCS_CKM.1 (4) Cryptographic Key Generation (SSH DSA Asymmetric Key Pair)*

FCS_CKM.1.1(4) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **DSA** and specified cryptographic key sizes **512 bit** that meet the following: **DSA FIPS 186-2.**

#### *6.2.2.5 FCS_CKM.1 (5) Cryptographic Key Generation (SSH Symmetric Key Derivation)*

FCS_CKM.1.1(5) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **SSH KDF** and specified cryptographic key sizes **128 bit (AES-128, cast128, RC4), 168 bit (TDES)**, **192 bit (AES-192)** and **256 bit (AES-256)** that meet the following: SSH v2 standard.

#### *6.2.2.6 FCS_CKM.2 (1) Cryptographic key distribution (SSL – RSA Public Keys)*

FCS_CKM.2.1 (1) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **digital certificates for public RSA keys** that meets the following: **certificate format as defined in the standard X.509 Version 3.**

*Application note - This requirement addresses the exchange of public RSA keys as part of the SSL client and server authentication / DH protocol.*

#### *6.2.2.7 FCS_CKM.2 (2) Cryptographic key distribution (SSL – DH Symmetric Key Agreement)*

FCS_CKM.2.1 (2) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **Secure Socket Layer key agreement** that meets the following: **SSL Version 3 (Internet Draft dated November 1996, Netscape Communication)**.

*Application Note This requirement addresses the distribution aspect of SSL session key agreement.*

#### *6.2.2.8 FCS_CKM.2 (3) Cryptographic key distribution (SSH – DH Symmetric Key Agreement)*

FCS_CKM.2.1 (3) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **Secure Shell diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha1 key agreement** that meets the following: **RFC 4253, RFC 4419**

#### *6.2.2.9 FCS_CKM.2 (4) Cryptographic key distribution (SSH – DSA Public Keys)*

FCS_CKM.2.1 (4) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **Digital Certificates for public DSA keys**

[3] The SSL Protocol Version 3.0, http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt.

that meets the following: **ssh-dss[4] key format as defined in Specification in Internet Draft: SSH Transport Layer Protocol (draftietf-secsh-transport-15.txt)**.

#### *6.2.2.10 FCS_CKM.4 Cryptographic key destruction*

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwrite method** that meets the following: **no standard.**

*Application Note: No formal key destruction method is followed for SNMPv3, SSHv2, SSLv2, and SSLv3. Keys are overwritten as new keys are loaded.*

#### *6.2.2.11 FCS_COP.1 (1) Cryptographic operation – SSL Session*

FCS_COP.1(1) The TSF shall perform **establishment of SSL/TLS Connections** in accordance with a specified cryptographic algorithm **RSA, triple-DES (in CBC mode), SHA-1, MD-5** and cryptographic key sizes [**1024 (for RSA) and 168 (for triple- DES)** that meet the following: **IETF RFC 2246**.

#### *6.2.2.12 FCS_COP.1 (2) Cryptographic operation – SSL Signing*

FCS_COP.1(2) The TSF shall perform **digital signature generation and digital signature verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024** that meet the following: **RSA PKCS#1**.

*Application note - This requirement addresses the RSA digital signature generation and verification operations using the RSA algorithm as required by the SSL session establishment protocol (provided a cipher suite including RSA is used). Note that the details of the signature format like the use of the PKCS#1 block type 1 and block type 2 are defined in the SSL Version 3 standard*.

#### *6.2.2.13 FCS_COP.1 (3) Cryptographic operation - Hashing*

FCS_COP.1(3) The TSF shall perform **secure hash (message digest) computation** in accordance with a specified cryptographic algorithm **HMAC-SHA1 and HMAC-MD5** and cryptographic key sizes **160 bits (HMAC-SHA1, HMAC-SHA1-96), and 128 bits (HMAC-MD5, HMAC-MD5-96)** that meet the following: **FIPS 198 and RFC 2104 HMAC-SHA1, RFC 1321 (MD5).**

#### *6.2.2.14 FCS_COP.1 (4) Cryptographic operation – SSH Session*

FCS_COP.1 (4) The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **TDES** and cryptographic key sizes **56, 112, and 168 bit** that meet the following: **SSH Version 2 standard[5] and the following cipher suite: 3des-cbc, aes128-cbc, blowfish-cbc, cast128-cbc, arcfour (RC4), aes192-cbc, aes256-256 as defined in the SSH v2 standard.**

#### *6.2.2.15 FCS_COP.1 (5) Cryptographic Operation – IPsec encryption services*

FCS_COP.1 (5) The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **TDES CBC or AES CBC** and cryptographic

[4] DSS is synonymous with the more widely used acronym DSA

[5] Internet Draft: SSH Transport Layer Protocol (draftietf-secsh-transport-15.txt)

key sizes **168 bits for TDES and 128, 192, 256 for AES** that meet the following **FIPS 46-3 for TDES and FIPS PUB 197 for AES.**

*Application note: Does not apply to 6400 or 6855 models.*

#### *6.2.2.16 FCS_COP.1 (6) Cryptographic Operation – SNMPv3 Encryption Services*

FCS_COP.1(6) The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm: **DES CBC** and cryptographic key sizes **56 bits** that meet the following: **FIPS PUB 46-3, RFC3414**.

### 6.2.3 Identification & Authentication (FIA)

#### *6.2.3.1 FIA_AFL.1(1) Authentication failure handling – Administrative-User*

FIA_AFL.1.1(1) The TSF shall detect when an administrator configurable positive integer within **the range 0 – 999**[6] unsuccessful authentication attempts occur related to **authentication attempts by an administrator configured to be authenticated locally by the TOE where the number of authentication attempts occurs during a configurable length of time**[7].

FIA_AFL.1.2(1) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **lock the administrator account for an administrator configurable length of time before being automatically unlocked**[8].

*Application Note: Account lockout does not apply to the default admin account*

#### *6.2.3.2 FIA_AFL.1(2) Authentication failure handling - Session*

FIA_AFL.1.1(2) The TSF shall detect when an administrator configurable positive integer within **the range 1 - 10** unsuccessful authentication attempts occur related to **authentication attempts by an administrator configured to be authenticated locally by the TOE during a TCP session**.

FIA_AFL.1.2(2) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **close the TCP session**.

#### *6.2.3.3 FIA_ATD.1 Administrative-user attribute definition*

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual administrative-users ***authenticated locally by the TOE***:

- **User ID**
- **Account Expiration Date**
- **Authentication data**
- **Role**

---

[6] A value of 0 means that the TSF will never disable user accounts due to failed login attempts.

[7] A value of 0 means that the TSF will count all failed login attempts and the configurable length of time is infinite. So, regardless of how much time is elapsed between failed logins, the TSF will count each consecutive failed login attempt.

[8] A value of 0 means that the TSF will not automatically unlock the user account.

#### *6.2.3.4 FIA_SOS.1 Verification of Secrets*

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the following administrator configurable conditions:**

- **a) Minimum password length between 8 and 14 characters;**
- **b) Password age of 1-150 days**
- **c) Password cannot contain username**
- **d) Password includes a minimum number of uppercase characters (the range is from 0-7 characters)**
- **e) Password includes a minimum number of lowercase characters (the range is from 0-7 characters)**
- **f) Password includes a minimum number of numeric characters (the range is from 0-7 characters)**
- **g) Password includes a minimum number of non-alphanumeric characters (the range is from 0-7 characters)**
- **h) Password must not be one of the previous passwords recorded (the range is 0-24 passwords recorded)**
- **i) Password must not be changed within a minimum number of days (the range is 0-150 days)**

#### *6.2.3.5 FIA_UAU_TRD.1 Timing of Authentication with a third party*

FIA_UAU_TRD.1.1 The TSF shall allow

- **Presentation of the CLI login prompt (for CLI users)**
- **Physical device authentication using IEEE 802.1X**
- **Information flows permitted for unauthenticated operators**

on behalf of the operator to be performed before the operator is authenticated by the TOE or the Operating environment as configured by the administrator.

FIA_UAU_TRD.1.2 The TSF shall require each operator to be successfully authenticated by the TOE or the Operating environment as configured by the administrator before allowing any other TSF-mediated actions on behalf of that operator**.**

#### *6.2.3.6 FIA_UID_TRD.1 Timing of Identification with a third party*

FIA_UID_TRD.1.1 The TSF shall allow

- **Presentation of the CLI login prompt (for CLI administrative-users)**
- **TOE port is enabled and set to an "unauthorized" state. (for 802.1X devices)**
- **Unauthenticated information flows**

on behalf of the operator to be performed before the user is identified by the TOE or the Operating environment as configured by the administrator.

FIA_UID_TRD.1.2 The TSF shall require each operator to be successfully identified by the TOE or the Operating environment as configured by the administrator before allowing any other TSF-mediated actions on behalf of that operator.

#### *6.2.3.7 FIA_UAU.5 Multiple authentication mechanisms*

FIA_UAU.5.1 The TSF shall provide **a password mechanism and certificate verification mechanism** to support administrative-user authentication.

FIA_UAU.5.2 The TSF shall authenticate any administrative-user's claimed identity according to the **following multiple authentication mechanism rules:**

- **Reusable password mechanism can be configured for administrators accessing the TOE.**
- **Keyed MAC can be used for IPsec communications.**

## 6.2.4 User Data Protection (FDP)

### *6.2.4.1 FDP_IFC.1 (1) Subset information flow control (Traffic Filter)*

FDP_IFC.1.1 (1) The TSF shall enforce the **Traffic Flow SFP** on.

Subjects: **physical network device**

Information: **IP packets**

Operation: **Permit or Deny the flow of information through the TSF**

### *6.2.4.2 FDP_IFF.1 (1) Simple security attributes (Traffic Filter)*

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

**Subject Security attributes:**

- **presumed network address of source subject;**
- **presumed MAC address of source subject;**
- **user network profiles**[9]

**Information security attributes:**

- **presumed network address of source subject;**
- **presumed MAC address of source subject;**
- **presumed network address of destination subject;**
- **presumed MAC address of destination subject;**
- **source port**
- **destination port**
- **transport layer protocol and their flags and attributes (UDP or TCP);**
- **TOE interface on which traffic arrives and departs;**
- **Assigned DHCP address if applicable.**

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

**a) Subjects on an internal network can cause information to flow through the TOE to another connected network 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;**
- **the presumed address of the source subject, in the information,**

[9] User network profiles provide the capability to assign users to "user roles" during authentication.

**translates to an internal network address;**

- **and the presumed address of the destination subject, in the information, translates to an address on the other connected network.**

**b) Subjects on the external network can cause information to flow through the TOE to another connected network 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;**
- **the presumed address of the source subject, in the information, translates to an external network address;**
- **and the presumed address of the destination subject, in the information, translates to an address on the other connected network**

FDP_IFF.1.3 (1) The TSF shall enforce the **following additional information flow control rules:**

- **c) The TOE shall drop requests for access or services where the presumed address of the source subject is not the same as the DHCP address assigned to that MAC address on that port.**

FDP_IFF.1.4 (1) The TSF shall explicitly authorize an information flow based on the following rules: **none.**

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

**a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed 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 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 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 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;**

#### *6.2.4.3 FDP_IFC.1 (2) Subset information flow control (VLAN)*

FDP_IFC.1.1 (2) The TSF shall enforce the **VLAN SFP** on.

Subjects: **physical network interfaces;**

Information: **IP packets**

Operation: **permit or deny layer two communication;**

#### *6.2.4.4 FDP_IFF.1 (2) Simple security attributes (VLAN)*

FDP_IFF.1.1 (2) The TSF shall enforce the **VLAN SFP** based on the following types of subject

and information security attributes:

**Subject security attributes:**

- **Receiving/transmitting VLAN interface;**
- **IP interface configuration (forward or not forward) for the VLAN**

**Information security attributes**

- **VLAN ID in Packet Header**
- **Logical Network identification (VLAN Tag)**

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:

**a) if the VLAN interfaces (subjects) are configured to be in the same VLAN ;**

**b) if the VLAN Tag (802.1Q) in the packet header is the same VLAN;**

**c) if an IP interface has been configured to forward on the VLANs, Layer-3 routing is allowed to transmit traffic between the VLANs.**

FDP_IFF.1.3 (2) The TSF shall enforce the **no additional rules**.

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) a VLAN does not have an IP interface configured to forward, packets associated with the ports associated with the VLAN will not be forwarded to ports in the other VLANs.**

**b) an IP interface is configured to not forward, packets received from hosts on other VLANs will not be forwarded.**

#### *6.2.4.5 FDP_RIP.1 Subset residual information protection*

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to, the following objects: **all objects**

### 6.2.5 Security Management (FMT)

#### *6.2.5.1 FMT_MOF.1 Management of security functions behavior*

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behavior of, disable, enable, modify the behavior of the functions **listed below** to **the authorized administrator**.

**a) Create, delete & modify all items corresponding to the Traffic Filter SFP & the VLAN SFP**

**b) Create, modify or delete users and all associated parameters.**

**c) Create, modify or delete routing table entries and routing protocol peers.**

**d) Enable, disable or configure use of remote identification/authentication servers (RADIUS/TACACS+/LDAP).**

**e) Configure Learned Port Security (LPS)[10]**

**f) Configuring IPsec**

**g) Terminating Another Administrator Session**

**h) Enable, disable, and configure audit parameters**

**i) Configure user login attempt lockout settings**

**j) Configure failed session login attempt settings**

**k) Configure password policy settings**

**l) Configure session timeout intervals**

#### *6.2.5.2 FMT_MSA.1 Management of security attributes*

FMT_MSA.1.1 The TSF shall enforce the **Traffic Filter SFP, VLAN SFP** to restrict the ability to change_default, query, modify, delete the security attributes **DHCP request, transport layer protocol, VLAN Tag** to **the authorized administrator**.

#### **6.2.5.3** ***FMT_MSA.3*** Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **Traffic Filter SFP, VLAN 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 **administrator** to specify alternative initial values to override the default values when an object or information is created.

#### *6.2.5.4 FMT_SMF.1 Specification of Management Functions*

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

**a) Modify and set the time & date**

**b) Query/view the audit trail**

**c) Create, delete & modify all items corresponding to the Traffic Filter SFP & the VLAN SFP**

**d) Create, modify or delete users and all associated parameters.**

**e) Create, modify or delete routing table entries and routing protocol peers.**

**f) Enable, disable or configure use of remote identification/authentication servers (RADIUS/TACACS+/LDAP).**

**g) Configure Learned Port Security (LPS)**

**h) Obtain and import digital certificates**

**i) Configuring IPsec**

**j) Terminating Another Administrator Session**

**k) Enable, disable, and configure audit parameters**

**l) Configure user login attempt lockout settings**

**m) Configure failed session login attempt settings**

[10] Learned Port Security (LPS) provides a mechanism for authorizing source learning of MAC addresses.

**n) Configure password policy settings**

**o) Configure session timeout intervals**

#### *6.2.5.5 FMT_SMR.1 Security roles*

FMT_SMR.1.1 The TSF shall maintain the roles **Authorized Administrator**

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

### 6.2.6 Protection of the TSF (FPT)

#### *6.2.6.1 FPT_STM.1 Reliable time stamps*

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

### 6.2.7 Trusted path/channels (FTP)

#### *6.2.7.1 FTP_ITC.1 Inter-TSF trusted channel*

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the TSF ***or*** another trusted IT product to initiate communication via the trusted channel.

*Application Note: The encryption used to protect the communication channel from disclosure is one of the symmetric algorithms specified in FCS_COP.1(5).*

*The secure hash algorithm used to provide detection of data modification transmitted through a communication channel is the algorithm specified in FCS_COP.1(3).*

*FTP_ITC.1.2 is used to ensure secure communications between the TOE and authorized IT entities (e.g., peer router).*

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **exchanging IP routing information**.

#### *6.2.7.2 FTP_ITC_PDR.1 Inter-TSF trusted channel: Use of Channel*

FTP_ITC_PDR.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_PDR.1.2 The TSF shall permit *another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC_PDR.1.3 The TSF shall use a trusted channel for the following functions **remote administration of the TOE via SSH or SSL.**

### 6.2.8 TOE Access (FTA)

#### *6.2.8.1 FTA_SSL.3 (1) TSF-initiated termination – login attempt session*

FTA_SSL.3.1 (1) The TSF shall terminate an interactive session after a **administrator-configurable number of seconds of inactivity during a login attempt**.

#### *6.2.8.2 FTA_SSL.3 (2) TSF-initiated termination – user session*

FTA_SSL.3.1 (2) The TSF shall terminate an interactive session after a **administrator-configurable number of minutes of inactivity during a user session**.

## 6.3 Security Functional Requirements for the Operational Environment

This section presents the SFRs for the operational environment that are taken from the CC Version 3.1 or from the extended components defined in Section 5. The operational environment shall satisfy the SFRs stated in the table below which lists the names of the SFR components. These requirements do not levy any additional requirements on the TOE itself, but rather on the operational environment. Following Table 9, the individual functional requirements are restated with any necessary operations completed.

| Functional Component ID | Functional Component Name |
|---|---|
| FIA_UAU_SRV.1 | Authentication via authentication server |
| FIA_UID_SRV.1 | Identification via authentication server |

Table 9: Security Functional Requirements for Operational Environment

### 6.3.1 FIA_UAU_SRV.1Authentication via authentication server

FIA_UAU_SRV.1.1 When invoked by the TSF, the **RADIUS, LDAP, or TACACS+ authentication servers** in the Operating environment shall determine if the operator has provided valid authentication data and pass the results of that determination back to the TOE.

### 6.3.2 FIA_UID_SRV.1 Identification via authentication server

FIA_UID_SRV.1.1 When invoked by the TSF, the **RADIUS, LDAP, or TACACS+ authentication servers** in the Operating environment shall determine if the operator has provided valid identification data and pass the results of that determination back to the TOE.

## 6.4 TOE Security Assurance Requirements

The Security assurance requirements (SARs) provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment). The table below identifies the security assurance requirements for the TOE drawn from CC Part 3: Security Assurance Requirements

| Assurance Class | Assurance Component ID | Assurance Component Name |
|---|---|---|
| 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: 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_FLR.2 | Flaw reporting procedures |
| ASE: Security Target evaluation | ASE_CCL.1 | Conformance claims |
| | ASE_ECD.1 | Extended components definition |
| | ASE_INT.1 | ST introduction |
| | ASE_OBJ.2 | Security objectives |
| | ASE_REQ.2 | Derived security requirements |
| | ASE_SPD.1 | Security problem definition |
| | ASE_TSS.1 | TOE summary specification |
| 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 10: Assurance Requirements: EAL2

## 6.5 Rationale For TOE Security Requirements

This section contains the security requirements rationale which includes a tracing that shows which SFRs address with TOE security objectives and justifications demonstrating that all TOE security objectives are addressed by the SFRs.

### 6.5.1 TOE Security Functional Requirements

| | O.ACCESS | O.AUDIT | O.AUDREV | O.MEDIATE | O.SELPRO | O.TOE_MGMT | O.TRANSIT | O.TIME |
|---|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | | x | | | | | | |
| FAU_SAR.1 | | | X | | | | | |
| FAU_STG.1 | | x | | | | | | |
| FCS_CKM.1 (1)-(5) | | | | | X | | | |
| FCS_CKM.2 (1)-(4) | | | | | X | | | |
| FCS_CKM.4 | | | | | X | | | |
| FCS_COP.1 (1)-(6) | | | | | X | | | |
| FIA_UID_TRD.1 | X | | | | | | | |
| FIA_UAU_TRD.1 | X | | | | | | | |
| FIA_AFL.1 | X | | | | | | | |
| FIA_UAU.5 | X | | | | | | | |
| FIA_ATD.1 | X | | | | | | | |
| FIA_SOS.1 | X | | | | | | | |
| FDP_IFC.1 (1)-(3) | | | | X | | | | |
| FDP_IFF.1 (1)-(3) | | | | X | | | | |
| FDP_RIP.1 | | | | X | | | | |
| FMT_MSA.1 | | | | | X | | | |
| FMT_MSA.3 | | | | | | X | | |
| FMT_MOF.1 | | | | | | X | | |
| FMT_SMF.1 | | | | | | X | | |
| FMT_SMR.1 | X | | | | | | | |
| FPT_STM.1 | | X | | | | | | X |
| FTA_SSL.3(1)-(2) | X | | | | | | | |
| FTP_ITC.1 | | | | | | | X | |
| FTP_ITC_PDR.1 | | | | | | | X | |

Table 11: SFR and Security Objectives Mapping

O.ACCESS The authorized administrator is required to authenticate to the TOE before access to any of the TOE management functions is allowed.

The administrator is required to provide their credentials, FIA_UID_TRD.1, and be authenticated, FIA_UAU_TRD.1, to the TOE. The Administrators login id,

| | |
|---|---|
| | password expiration and role (FMT_SMR.1) are stored and configured in the TOE if the administrator is setup to be authenticated locally by the TOE, FIA_ATD.1.<br><br>FIA_UAU.5 requires the TOE to provide two different authentication methods: password and HMAC.<br><br>FIA_AFL.1 exists to minimize guessing of authentication credentials by brute force method when configured to authenticate locally by the TOE. An administrator account is locked for a time duration specified by an authorized administrator when a predefined number of consecutive unsuccessful login attempts are reached.<br><br>FIA_SOS.1 exists to enforce password complexity requirements when a password is created or modified.<br><br>FTA_SSL.3(1)-(2) exists to provide a capability for the TSF to initiate termination of interactive operator sessions to protect against unauthorized use of an abandoned operator session. |
| O.AUDIT | The TOE will create a readable audit trail of security-related events, with accurate dates and times, for use by the administrator.<br><br>The TOE will generate an audit trail, FAU_GEN.1 of security relevant activities and store that information in the TOE, FAU_STG.1. The TOE will contain a hardware clock for the use of the TOE audit trail, FPT_STM.1 |
| O.AUDREV | The TOE will provide a mechanism for the administrator to review the audit trail.<br><br>The TOE provides the ability to review the audit logs, FAU_SAR.1. |
| O.MEDIATE | The TOE will meditate all network traffic as defined by the policies created by the administrator and ensure that residual information from a previous information flow is not available.<br><br>There are 2 SFPs enforced by the TOE, Traffic Filter SFP, FDP_IFC.1 (1) & FDP_IFF.1 (1) and VLAN SFP, FDP_IFC.1 (2) & FDP_IFF.1 (2). The TOE will also clear any information from its internal buffers prior to allowing any new information into those buffers, FDP_RIP.1 |
| O.SELPRO | The TOE will protect itself against attempts by unauthorized users to bypass, deactivate or tamper with TOE security functions<br><br>The TOE encrypts the traffic to and from the authorized administrator, with defined Key generation, FCS_CKM.1 (1), FCS_CKM.1 (2), FCS_CKM.1 (3), FCS_CKM.1 (4), FCS_CKM.1 (5), Key Distribution FCS_CKM.2 (1), FCS_CKM.2 (2), FCS_CKM.2 (3), FCS_CKM.2 (4) Key Destruction, FCS_CKM.4, secure values, FMT_MSA.1, and Cryptographic operations FCS_COP.1 (1), FCS_COP.1 (2). FCS_COP.1 (3), FCS_COP.1 (4), FCS_COP.1 (5) and FCS_COP.1 (6). |

| | |
|---|---|
| O.TOE_MGMT | The TOE will provide interfaces to allow the administrator to configure the other security functions of the TOE, including configuring policies to mediate traffic.<br><br>These functions will be defined, FMT_SMF.1, and the administrators abilities with regard to modify those functions will also be defined, FMT_MOF.1<br><br>In addition, the TOE provides the authorized administrator the ability to modify the default values of the 2 SFPs, FMT_MSA.3. |
| O.TRANSIT | The TSF shall protect TSF data when it is in transit between the TSF and a remote trusted IT entity.<br><br>FTP_ITC.1 and FTP_ITC_PDR.1 ensure protection of the communication between the TOE and trusted IT entities while transmitting data. |
| O.TIME | The TOE will provide a time stamp for its own use.<br><br>The TOE will contain a hardware clock for the use of the TOE, FPT_STM.1. |

### 6.5.2 TOE Security Assurance Requirements

The chosen assurance level, EAL2, is consistent with the postulated threat environment. EAL2 was chosen to provide a moderate to high level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. Additionally, the product vendor has specific customer requests for the evaluation of the TOE at this assurance level. These potential customers of the product vendor have determined for their own networks that an EAL2 evaluation of the product will provide satisfactory assurance.

EAL2 is augmented with ALC_FLR.2 to assist in ensuring that discovered security flaws are tracked and are corrected by the developer and that TOE users are aware of how to report a security flaw and receive corrective fixes.

## 6.6 Rationale For IT Security Requirement Dependencies

This section includes a table of the requirements are their dependencies and a rational for any dependencies that are not satisfied.

| Functional Component | Dependency | Included |
|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | Yes |
| FAU_SAR.1 | FAU_GEN.1 | Yes |
| FAU_STG.1 | FAU_GEN.1 | Yes |
| FCS_CKM.1 (1) | FCS_CKM.2 or<br>FCS_COP.1<br>FCS_CKM.4 | Yes |
| FCS_CKM.1 (2) | FCS_CKM.2 or<br>FCS_COP.1<br>FCS_CKM.4 | Yes |
| FCS_CKM.1 (3) | FCS_CKM.2 or<br>FCS_COP.1<br>FCS_CKM.4 | Yes |

| Functional Component | Dependency | Included |
|---|---|---|
| FCS_CKM.1 (4) | FCS_CKM.2 or FCS_COP.1<br>FCS_CKM.4 | Yes |
| FCS_CKM.1 (5) | FCS_CKM.2 or FCS_COP.1<br>FCS_CKM.4 | Yes |
| FCS_CKM.2 (1) | FCS_CKM.1<br>FCS_CKM.4 | Yes |
| FCS_CKM.2 (2) | FCS_CKM.1<br>FCS_CKM.4 | Yes |
| FCS_CKM.2 (3) | FCS_CKM.1<br>FCS_CKM.4 | Yes |
| FCS_CKM.2 (4) | FCS_CKM.1<br>FCS_CKM.4 | Yes |
| FCS_CKM.4 | FCS_CKM.1 | Yes |
| FCS_COP.1 (1) | FCS_CKM.1<br>FCS_CKM.4 | Yes |
| FCS_COP.1 (2) | FCS_CKM.1<br>FCS_CKM.4 | Yes |
| FCS_COP.1 (3) | FCS_CKM.1<br>FCS_CKM.4 | Yes |
| FCS_COP.1 (4) | FCS_CKM.1<br>FCS_CKM.4 | Yes |
| FCS_COP.1 (5) | FCS_CKM.1<br>FCS_CKM.4 | Yes |
| FCS_COP.1 (6) | FCS_CKM.1<br>FCS_CKM.4 | Yes |
| FIA_UID_TRD.1 | None | |
| FIA_UAU_TRD.1 | FIA_UID.1 or FIA_UID_TRD.1 or FIA_UID_SRV.1 | Yes |
| FIA_UAU.5 | None | |
| FIA_AFL.1 | FIA_UAU.1 | Yes, via FIA_UAU_TRD.1 |
| FIA_ATD.1 | None | |
| FIA_SOS.1 | None | |
| FDP_IFC.1 (1) | FDP_IFF.1 (1) | Yes |
| FDP_IFF.1 (1) | FDP_IFC.1 (1)<br>FMT_MSA.3 | Yes |
| FDP_IFC.1 (2) | FDP_IFF.1 (2) | Yes |
| FDP_IFF.1 (2) | FDP_IFC.1 (2)<br>FMT_MSA.3 | Yes |
| FDP_RIP.1 | None | |
| FMT_MOF.1 | FMT_SMF.1<br>FMT_SMR.1 | Yes |

| Functional Component | Dependency | Included |
|---|---|---|
| FMT_MSA.1 | FDP_IFC.1<br>FMT_SMR.1<br>FMT_SMF.1 | Yes |
| FMT_MSA.3 | FMT_SMR.1<br>FMT_MSA.1 | Yes |
| FMT_SMF.1 | None | |
| FMT_SMR.1 | FIA_UID.1 | Yes, via FIA_UID_TRD.1 |
| FPT_STM.1 | None | |
| FTA_SSL.3 (1) | None | |
| FTA_SSL.3 (2) | None | |
| FTP_ITC.1 | None | |
| FTP_ITC_PDR.1 | None | |

Table 12: SFR Dependencies

# 7 TOE Summary Specification

This section presents a description of how the TOE SFRs are satisfied, organized by security function.

## 7.1 Security Audit

### 7.1.1 Audit Generation: FAU_GEN.1

The TOE satisfies the security audit generation requirement via the Switch Logging and QoS Logging features. Switch Logging records the audit events for all administrative operations performed. QoS logging records the audit events for the information flow rule decisions made by the Traffic Filter SFP.

Both Switch logging and QoS Logging send the log messages to the switch logging utility, which is an event logging application on the OmniSwitch.

Both logging mechanisms support severity levels identified in the following table. Level 6, 'Info' is enabled for all events by default.

| Supported Levels | Numeric Equivalents | Description |
|---|---|---|
| Alarm | 2 | Highest severity. The system is about to crash and reboot |
| Error | 3 | System functionality is reduced |
| Alert | 4 | A violation has occurred |
| Warning | 5 | A unexpected, non-critical event has occurred |
| Info | 6 | Any other non-debug message (default). |
| Debug1 | 7 | A normal event debug message. |
| Debug2 | 8 | A debug-specific message |
| Debug3 | 9 | Lowest severity. A maximum verbosity debug message. |

#### *7.1.1.1 Switch Logging*

The TOE generates audit messages for all administrative operations performed, including enabling and disabling auditing (both Switch Logging and QoS Logging). Audit events are detected based on administrative-user-initiated actions.

The CLI and SNMP interfaces generate the audit messages based on administrative-user-initiated events.

Each audit record contains the date and time of the event, type of event, subject identity and outcome (success or failure). The type of event and outcome are included in the Log Message field which specifies the condition recorded.

Using CLI or SNMP, it is possible to change, either globally for all Applications or on a per Application basis, the level of logging that occurs.

When an audit event request is made, the severity level on the request is compared to the severity level assigned to the application id for which the event occurs. If the severity level of the log request is less than or equal to that of the application id, the log message is generated and placed in the log file.

The administrator is instructed to configure the switch log to include CLI and SNMP logging events.

#### *7.1.1.2 QoS Logging*

QoS[11] logging is implemented by configuring the switch to log information about flows coming through the switch that match a specified rule policy. The rule is configured to enable or disable logging for flows that match the rule and to specify the severity level of the event associated with the rule.

Using CLI or SNMP, the administrator has the ability to configure the level of log detail included in the audit records and to change the types of messages which are logged. The type of events that may be logged includes the following:

- Events for rules configured on the switch
- Layer 2 QoS events
- Layer 3 QoS events

### 7.1.2 Audit Log Review: FAU_SAR.1

The TOE provides a CLI interface to review audit logs.

The audit records stored in the Switch Logs can be searched by session id, date & time, security level, and application id.

The format of the audit records in the Switch Log is as follows:

[Time Stamp] [Application ID] [Security Level] [Log Message]

The format of the audit records in the QoS Log that are recorded as a result of security rules is as follows:

Each entry in the QoS log is 4 lines long. Each line begins with a date and time stamp.

The first line identifies the time of the event, the rule matched, the action taken (drop or accept) and the slot/port, if applicable.

The second line identifies the packet as Tagged or DoubleTagged for VLAN and identifies the associated ports.

The third line records the source and destination MAC addresses.

The fourth line identifies the protocol, ports, IP addresses specific to the IPv6 or IPv4 traffic.

### 7.1.3 Audit Storage: FAU_STG.1

For each log type, the switch logging utility can be configured to send audit records to a log file on the switch's flash file system, displayed on the switch console, and/or to a remote syslog server. In the evaluated configuration, the TOE is configured to write the logs to a text file stored in the flash file system.

The TOE writes audit messages to logs stored in the systems flash memory for permanent storage.

For Switch logging, it is possible for the administrator to increase the total size of the log file from a minimum of 32k to the free space of the flash drive. Once the files are full the oldest entries are overwritten. The TOE requires that authorized administrators be identified and authenticated prior to accessing security-related functions that control the stored audit data. The TOE can be configured to send the syslog files containing the switch logging output to a maximum of four external syslog servers.

For QoS logging, it is possible for the administrator to configure the number of lines contained in the QoS log.

### 7.1.4 Reliable Time Stamps: FPT_STM.1

The TOE has an internal system clock which is used to generate timestamps for the TOE's own use. The

[11] QoS is a term that is used to refer to the manipulation of information flows coming through the switch based on administrator defined policies.

reliable time stamps are used to generate useful, interpretable audit records.

## 7.2 Cryptographic Operations

The TOE uses cryptographic operations to protect communications between itself and external trusted IT entities.

The cryptography used in this product has not been FIPS 140-2 certified nor has it been analyzed or tested to confirm to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The following table demonstrates the secure communication protocols and algorithms used by the TOE to provide secure communication between the TOE and remote trusted IT entities:

| **Protocol / Algorithm** | **Use** |
|---|---|
| SSLv2<br>SSLv3 | End-User Authentication<br>▪ Captive Portal<br>▪ LDAP |
| SSHv2<br>SFTP | Remote Management<br>▪ CLI<br>▪ Secure File Transfer (SFTP) |
| SNMPv3 | SNMPv3 confidentiality and integrity |
| IPsec | Exchange of IP route information with external routers on IPv6 |
| HMAC-MD5<br>HMAC-SHA1 | IPsec message authentication<br>Administration authentication traffic using RADIUS, LDAP & TACACS+ (SNMPv3)<br>End-User Authentication<br>▪ MAC-based authentication using RADIUS<br>▪ Captive Portal |
| HMAC-MD5 | OSPF with IPv4 routing information |

The SSLv2, SSLv3, and SSHv2 protocols allow for secure communication between the TOE and a remote trusted product over an insecure network for the purposes of remote administration.

For SSH, the TOE uses Diffie-Hellman to establish a secure session for administrative-user authentication. Once the administrative-user is successfully authenticated, a command line shell is initiated over the secured session. The transmitted data is encrypted to provide confidentiality. Administrative-users obtain access to a command line shell or secure file transfer from the remote system. For SFTP, instead of initiating a command line shell over the secure session, the file transfer program is executed. The SSHv2 implementation is based on Open SSH version 2.9p2.

For SSL, the TOE establishes a secure communication path with the remote trusted product without operator authentication, but with certificate-based authentication of the client system (remote trusted product) if so configured. The server side (TOE) of the SSL session is authenticated using a digital certificate. The transmitted data is encrypted to provide confidentiality. A message authentication code (MAC) is generated for the transmitted data. This MAC is transmitted with the data to ensure integrity of the transmitted data and provide the ability to detect modifications to the transmitted data. SSL can

resend data if modifications are detected. The SSLv2 and SSLv3 implementations are based on the RSA SSL C Library.

IPsec is a framework of open standards used to provide private, secure network communications over IP networks. The cryptographic operations used are determined by the IPsec Security Association (SA) which is defined by the packet's destination IP address, a security protocol (e.g., encryption/authentication types and keys), and a unique identification value, called a Security Parameter Index (SPI). The SA associates the security services and a key with the network packets being protected. The TOE only implements manual IPsec key management (IKE is not implemented), so the administrator is responsible for creating the SAs. The IPsec implementation supports the following modes of operations:

- ESP confidentiality and integrity
- ESP confidentiality and AH authentication

By default, the TOE enforces the use of secure cryptographic security attributes.

### 7.2.1 Key Generation: FCS_CKM.1(1)-(5)

The TOE supports 5 different types of key generation methods.

The TOE generates asymmetric cryptographic keys that are used to protect communications for SSLv2 and SSLv3 remote administration. The keys are generated in accordance with the RSA algorithm and are 1024 bit key size.

The TOE generates symmetric cryptographic session keys as defined by the SSLv3 standard for SSLv2 and SSLv3 remote administration. These symmetric keys can have a key size of 128 bit for RC4, 168 bit for Triple DES (TDES), and 128 bit or 256 bit for AES.

The TOE generates symmetric cryptographic keys used for SNMPv3 authentication and privacy (encryption). These 56 bit keys are generated in accordance with USM for SNMPv3 RFC3414.

The TOE generates an asymmetric cryptographic key pair used to protect communications for SSHv2 remote administration. This key pair is generated in accordance with the DSA algorithm with a 512 bit key size. These keys can be replaced by the administrator once installed.

The TOE generates symmetric cryptographic session keys as defined by the SSHv2 standard for SSHv2 remote administration. These symmetric keys can have a key size of 128 bit or 256 bit for RC4 (Arcfour), 128 bit for Cast, 128 bit for Blowfish, 168 bit for Triple DES (TDES), and 128 bit or 256 bit for AES (Rijndael).

### 7.2.2 Key Distribution: FCS_CKM.2(1)-(4)

The TOE supports 4 different types of key distribution methods.

The TOE implements the exchange of public RSA keys as part of the SSL client and server authentication for SSL remote administration.

The TOE implements SSL session key agreement as part of the SSL handshake protocol for SSL remote administration.

The TOE implements Diffie-Hellman session key agreement to establish cryptographic keys used for SSHv.2 remote administration.

The TOE implements Digital Certificates for public DSS key exchange to distribute cryptographic keys used for SSHv.2 remote administration.

The TOE implements manual key exchange for IPsec.

### 7.2.3 Key Destruction: FCS_CKM.4

The TOE destroys session keys used for SSH and TLS/SSL by clearing and deallocating the RAM memory used to store the session key, and destroys all other cryptographic keys stored by the TOE by

overwriting an old key with new key.

### 7.2.4 Cryptographic Operations: FCS_COP.1(1)-(6)

The TOE implements encryption and decryption of data exchanged during the establishment of SSL connections. The TOE uses RSA, Triple DES (in CBC mode), SHA-1, and MD5 to implement the SSL session establishment with key sizes of 1024 for RSA and 168 for TDES. These cryptographic algorithms provide for confidentiality and integrity of the SSL session establishment.

The TOE implements signing of a server-generated authentication challenge and signing of resource hash during SSL session establishment. This ensures data transmitted from one endpoint arrives unaltered on the other endpoint, providing integrity of the data transmitted. The TOE implements the RSA algorithm with a key size of 1024 to provide this capability.

The TOE implements secure hashing of communications with external authentication servers and communications to perform end-user authentication using MAC authentication and Captive Portal. This ensures data transmitted from one endpoint arrives unaltered on the other endpoint, providing integrity of the data transmitted. The TOE uses HMAC-SHA1 or HMAC-MD5 to perform IPsec message authentication (data integrity and authenticity of a message). The TOE implements HMAC-SHA1 with a 160 bit key and HMAC-MD5 with a 128 bit key. OSPF with IPv4 routing information is integrity checked on a per-message basis with HMAC-MD5. The TOE uses HMAC-MD5-96 (using a 128 bit key) or HMAC-SHA-96 (using a 160 bit key) to perform SNMPv3 data integrity and data origin authentication.

The TOE implements encryption and decryption of data exchanged during remote TOE CLI administration (SSH or SFTP) which provides confidentiality of the data transmitted. The TOE implements TDES with a 168 bit key.

The TOE implements encryption and decryption of IPsec packet flows passing through untrusted networks using TDES with a 168 bit key and/or AES CBC mode with a 128, 192, or 256 bit key.

The TOE implements encryption and decryption of data during exchange of SNMPv3 messages using DES with a 56 bit key.

## 7.3 Identification and Authentication

There are two types of authentication performed by the TOE: Authorized Administrator Authentication and End-user Authentication. (The term end-user refers to the device on the network generating or receiving network traffic; the term administrative-user refers to authorized administrators; the term operator is used when the context is neutral to either end-user or administrative-user.)

### 7.3.1 Timing of Identification and Authentication: FIA_UAU_TRD.1, FIA_UID_TRD.1, FIA_UAU.5

The TOE requires administrators and end-users to be identified and authenticated prior to accessing all security-related functions.

The TOE requires the administrator to identify and authenticate to the TOE prior to accessing any of the management functionality regardless of the mechanism being used to interface with the TOE (via the serial console, SSH, SFTP, SNMPv3, SSL). Administrator authentication can be performed locally on the TOE or the TOE can send a request to external authentication server in the operational environment to verify the identity of the operator. The method of authentication required by the TOE is configured based on the interface used to access the TOE. The external authentication servers supported by the TOE for administrator authentication are LDAP, RADIUS, and TACACS+. (The LDAP, RADIUS and TACACS+ external authentication servers are stored in the operating environment.)

General (non-security related) network traffic may be authenticated or unauthenticated. Unauthenticated general network traffic corresponds to the “unauthenticated information flows” cited in FIA_UID_TRD.1.1.

End-user (device) authentication is used to mediate network information flows. The end-user authentication is performed by verifying the credentials of either the device or the end-user operating the

device. The TOE supports three types of end-user authentication: MAC authentication, web-based authentication (Captive Portal), and IEEE 802.1X. These authentication methods require an external authentication server in the operational environment. The TOE dynamically assigns the appropriate authentication mechanism to each network device at the port level. Regardless of what is connected to a switch port (hubs, IP phones, etc.), every device is identified and authenticated. For example, when managed devices that are capable of 802.1X authentication attempt to connect to the network they will be challenged to provide their credentials. Other legacy devices such as printers will not be challenged, but instead will be granted access through MAC authentication. Likewise, guests or devices unknown to the network will be directed to provide authentication credentials using a Web-based interface. Once configured, the security workflow operates with minimal administrator intervention.

The TOE provides MAC authentication which verifies the identity of the end-user (device) by creating a request for a RADIUS server to verify the MAC address.

The TOE provides web-based authentication (Captive Portal) which allows end-users to authenticate using their credentials. It does so by intercepting all traffic from the MAC address and diverting the end-user's web browser to a web page internal to the TOE. The TOE will then verify the credentials entered on the web page against an external RADIUS server.

For 802.1X device authentication, upon detection of the supplicant, access to the TOE is enabled and set to an "unauthorized" state. In this state, only 802.1X traffic from the device is allowed; other network traffic is blocked. Next, the TOE sends out the EAP-Request identity to the supplicant, the supplicant responds with the EAP-response packet that the authenticator forwards to the RADIUS authentication server in the TOE operating environment. If the RADIUS server accepts the request, the TOE sets the port to the "authorized" mode and normal traffic is allowed. When the supplicant ends its session, it sends an EAP-logoff message to the TOE. The TOE then sets the port to the "unauthorized" state thereby blocking all non-EAP traffic.

NOTE: 802.1X is the recommended solution to provide the highest level of security for end-user authentication.

The TOE also implements HMAC and AES CBC for use in authentication in the IPsec protocol. The TOE only implements manual key management, so the administrator is responsible for creating the SAs which define the algorithms and the authentication method used and the keys used. The IPsec protocol is only used for exchange of IP route information with external routers on IPv6.

### 7.3.2 User Attribute Definition: FIA_ATD.1

When configured for local authentication, the TOE maintains administrative-user security attributes of identifier (User ID), password information (authentication data), and user privileges (authorizations or user profile) and roles. The authentication data is hashed prior to being stored. These attributes are stored locally on the flash file system. All references to "user" in this section refer to administrative-user accounts and associated attributes,

There is one default user account provided with the TOE: admin. The admin user account is the initial administrator assigned all privileges. The admin user account is used to install and setup the TOE.

The TOE also provides a default user configuration used to store user defaults for assigning privileges and profile information to newly created users. The default user configuration cannot be used to log into the switch.

When an external authentication server is used, the external authentication server is responsible for storing, maintaining, and communicating the user's security attributes.

### 7.3.3 Authentication Failure Handling: FIA_AFL.1(1)-(2)

The TOE provides two different authentication failure methods: session-based and user-based. All references to "user" in this section refer to administrative-user accounts and associated attributes,

For session-based authentication failure handling, the TOE tracks the authentication failures per TCP session, regardless of user. If the number of failed user login attempts exceeds the number of allowed failed login attempts per TCP session, the TOE closes the TCP session. The session failed login attempt

counter is reset when a new TCP session starts.

For user-based authentication failure handling, the TOE provides the following user authentication failure settings:

| | |
|---|---|
| Lockout window | The length of time a failed user login attempt is aged before it is no longer counted as a failed user login attempt. The valid range is 0 to 99,999. The number of failed login attempts is decremented by the number of failed attempts that age beyond the lockout window. The default lockout window is set to 0, which means that all consecutive failed login attempts are counted, regardless of how much time has elapsed between the failed logins. |
| Lockout threshold | The number of failed user login attempts allowed within a given lockout window period of time (0-999). The default lockout threshold is set to 0, which means that there is no limit to the number of failed login attempts allowed. |
| Lockout duration | The length of time a user account remains locked out until it is automatically unlocked. The valid range is 0 to 99,999. The default lockout duration is set to 0, which means that there is no automatic unlocking of a user account by the switch. |

When authentication is performed locally by the TOE, the TOE ensures that if the number of failed user login attempts exceeds the lockout threshold during the lockout window period of time, the user account is locked out of the switch for the lockout duration. The user's authentication failure counter is reset when the user successfully authenticates. Account lockout does not apply to the default admin account on the switch.

When an external authentication server is used, the external authentication server is responsible for locking out the user.

### 7.3.4 Password Restrictions: FIA_SOS.1

The TOE provides global password settings used to implement and enforce local password complexity when a password is created or modified. All references to "user" in this section refer to administrative-user accounts and associated attributes, The global password settings are configured by the administrator. The password settings available on the TOE are:

| | |
|---|---|
| Minimum Password Length | The number of characters required when configuring a user password. The default is 8 characters and the allowed range is 1 - 14 characters. The administrator is instructed to configure this value to be in the range of 8 - 14 characters. |
| Password Expiration | The number of days before user passwords will expire. The allowed range is 1 - 150 days. Password expiration is disabled by default. |
| Username not allowed | Specifies whether or not the password is allowed to contain the username. The default is to allow the password to contain the username. |
| Minimum Uppercase characters | Specifies the minimum number of uppercase characters required for a user password. The allowed range is 0 - 7. By default, there is no required minimum number of uppercase characters. |

| | |
|---|---|
| Minimum Lowercase characters | Specifies the minimum number of lowercase characters required for a user password. The allowed range is 0 - 7. By default, there is no required minimum number of lowercase characters. |
| Minimum Numeric characters | Specifies the minimum number of numeric characters (base-10 digits) required for a user password. The allowed range is 0 - 7. By default, there is no required minimum number of numeric characters. |
| Minimum Non-alpha characters | Specifies the minimum number of non-alphanumeric characters (symbols) required for a user password. The allowed range is 0 - 7. By default, there is no required minimum number of non-alphanumeric characters. |
| Password History | Specifies the maximum number of old passwords to retain. The range is 0 - 24 and the default is to retain 4 old passwords. The user is prevented from reusing any retained passwords. A value of 0 disables the password history function. |
| Minimum Password Age | Specifies the minimum number of days during which the user is prevented from changing a password. The allowed range is 0 - 150. By default, there is no required minimum number of days. |

### 7.3.5 Session Timeout: FTA_SSL.3

The TOE provides two different session timeout capabilities: login attempt session timeout and user session timeouts. All references to “user” in this section refer to administrative-user accounts and associated attributes, The login attempt session timeout defines the amount of time the user can take to accomplish a successful login to the switch. If the login timeout period is exceeded, the TCP connection is closed by the switch. The default login timeout period is 55 seconds. The user session timeouts define the amount of time the user can be inactive for CLI (console) and SFTP sessions. When the TOE detects no user activity for the administrator configured period of time, the user is logged off the TOE. The default timeout for CLI and SFTP sessions is four minutes.

## 7.4 Traffic Mediation

The TOE provides two different types of traffic mediation: VLANs and Traffic Filtering. All references to “user” in this section refer to end-users,

### 7.4.1 VLAN Flow Control: FDP_IFC.1(2), FDP_IFF.1(2)

The TOE controls the bridging of frames received and imposes a security policy (VLAN) to restrict them.

When a packet is received on a port, the port’s VLAN ID is inserted into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID.

Packets may have a Logical Network identification (VLAN Tag) associated to them indicating which VLAN they are a member of. This method allows the switch to bridge traffic for multiple VLANs over one physical port connection. The TOE will enforce VLAN separation by only allowing packets onto the VLAN that matches the VLAN Tag. VLAN traffic will not be forwarded to interfaces not in that VLAN.

A web browser client authenticates using IP to a predetermined interface and VLAN on the switch. An Authentication agent in the switch communicates with the authentication server in the Operating Environment (RADIUS) to carry out the authentication process.

If a device needs to communicate with another device that belongs to a different VLAN, the TOE mediates the flow of information between the VLANs using IP forwarding (i.e., routing). This forwarding

function is based on internal routing tables. These routing tables are processed top-down, with processing continuing until the first match is made. The routing table may be statically updated by a privileged administrator or dynamically through routing protocols. The following routing protocols are permitted:

IPV4 Routing Protocols: OSPF / RIPv2 / BGP / VRRP / VRRP2

IPV6 Routing Protocols: OSPFv3 / RIPng / VRRP3

### 7.4.2 Traffic Filtering: FDP_IFC.1(1), FDP_IFF.1(1)

Once the TOE is assigned to a VLAN, the TOE can filter packets based on the security attributes of subject and IP packet. When a flow comes into the switch, the switch checks if there are any policies that match the conditions of the flow. If there are no policies that match the flow, the flow is permitted or denied based on the global disposition value. By default, the TOE is configured to permit (route) all packets that do not match a policy. The global disposition value can be changed by the administrator.

The TOE controls the layer2 and layer3/4 traffic that is allowed to flow through the TOE, imposing a security policy to filter the traffic. Traffic is filtered using Access Control Lists (ACLs) stored in the policy database. The TOE examines each network packet received to determine whether to route or drop the packet based on the rules specified by the administrator in the ACLs. The rules in the ACL can be based on source IP address, destination IP address, source MAC address, destination MAC address, source port, destination port, the transport layer protocol, and the user network profile. The TOE rejects packets arriving on a network interface if the presumed address of the source belongs to a different network interface, providing the ability to reject known spoofed IP addresses.

The policies are assigned precedence which defines the order in which the rules are checked and what actions are taken if there is a conflict. If a flow matches more than one policy, the policy with the highest precedence is applied to the flow. If a flow matches more than one policy with the same precedence values, the rule configured first takes precedence.

Rules can also be configured to enable logging of use of the rule and to define the severity level assigned to the event.

User network profiles allow administrators to define access control for user groups. Access to network resources is based on a user's profile instead of a MAC address, IP address or port thereby simplifying the configuration of the network while allowing for increased end station mobility. The profiles are then linked to the appropriate access control, allowing an administrator to define what resources are available to a group of users, regardless of source subnet, VLAN or other characteristics.

### 7.4.3 Residual Information Protection: FDP_RIP.1

The TOE ensures that residual information is unavailable to other resources by overwriting areas of memory that store any incoming packet data.

When packets arrive on the TOE's network interface they are written into memory. The TOE overwrites information previously stored in that memory location with the newly received packet. Pointers are used by AOS to identify the beginning and ending of each packet in memory. The correct use and operation of these pointers ensures that data from a prior packet stored in memory is not inadvertently included in a later packet or available for use.

## 7.5 Security Management

The Alcatel-Lucent OmniSwitch provides 3 different interfaces each providing a comprehensive set of security management capabilities for the TOE: CLI or SNMP. The CLI can be accessed from the serial console or an SSH connection. In addition, the Flash file system on the switch provides the ability to store and edit configuration files that can be transferred to and from the Flash file system via SFTP. All references to "user" in this section refer to administrative-users,

### 7.5.1 Security Management Functions: FMT_MOF.1, FMT_SMF.1

The CLI and SNMP external interfaces provide the following management functions for use by the authorized administrator:

- Modify and set the time & date
- Create, delete & modify all items corresponding to the Traffic Filter SFP & the VLAN SFP
- Create, modify or delete users and all associated parameters.
- Create, modify or delete routing table entries and routing protocol peers.
- Enable, disable or configure use of remote authentication servers (RADIUS/TACACS+/LDAP).
- Configure Ethernet Ports
- Configure Learned Port Security (LPS)
- Configuring IPsec
- Terminating Another Administrator Session
- Enable, disable and configure audit parameters
- Configure user login attempt lockout settings
- Configure failed session login attempt settings
- Configure password policy settings
- Configure session timeout intervals

The CLI provides an interface for querying/viewing the audit trail.

SFTP is used to obtain and import digital certificates

SNMPv3 can be used to retrieve tables to obtain configuration settings and statistics, but it cannot be used to obtain information stored in files, such as audit data.

Acting on behalf of the authorized administrator, the CLI and SNMP interfaces request security management operations from the same underlying service in the TOE. Therefore, although there are 3 different methods of use for requesting the security management functions, each method utilizes the same underlying software to actually perform the functions.

Use of each of these management functions is restricted to the authorized administrator by requiring the administrator to successfully identify and authenticate to the TOE prior to allowing access to the functions. In addition, users are assigned read-only or read-write access to the command families available on the switch. The command families correspond to the commands categories available via the 3 interfaces. Examples of command families include file, system, config, module, interface, ip, vlan, dns. qos, policy, session, aaa.

### 7.5.2 Security Attribute Management: FMT_MSA.1 & FMT_MSA.3

The TOE restricts all management of the information security attributes in the DHCP request, transport layer protocol, VLAN Tag SFPs to the authorized administrator.

The associated global disposition value determines the default values for security attributes used by the information flow SFPs. By default, the TOE is configured to permit (route) all packets that do not match a policy. The global disposition values can be changed by the administrator. The administrator is instructed in administrator guidance to set default attribute values in a secure manner as necessary for the deployed environment.

### 7.5.3 Security Roles: FMT_SMR.1

There is a single role of Administrator for the TOE. Administrators are granted access to management functions based on the access granted to their user account. The TOE provides the ability to grant read-

only or read-write access to the command families available on the switch. The command families correspond to the commands categories available via the 3 interfaces. Examples of command families include file, system, config, module, interface, ip, vlan, dns, qos, policy, session, aaa. The aaa command family provides the ability to configure the type of authentication methods supported by the switch and perform user account management.

## 7.6 Protection of the TOE

### 7.6.1 Trusted Channels: FTP_ITC.1 & FTP_ITC_PDR.1

The TOE implements IPsec to provide a trusted communication channel for communicating between the TOE and authorized IT entities (e.g., obtaining routing information from a peer router). The TOE implementation of IPsec supports the transport mode of operation where only the data transferred in the IPv6 packet (payload) is encrypted and/or authenticated. Refer to Section 7.2 for a summary of IPsec and the associated cryptographic support measures implemented by the TOE. OSPF with IPv4 routing information is integrity checked on a message basis with HMAC-MD5.

The TOE provides a trusted communication channel for remote administration via SSH v2, SSLv2, and SSL v3 depending upon the TSFI used to interface with the TOE. Refer to Section 7.2 for a summary of SSL, SSH, and the associated cryptographic support measures implemented by the TOE.