Hewlett Packard Enterprise
HSR6600 Series, HSR6800 Series and MSR1000 Series Routers
Security Target

Version 1.0
March 10, 2016

Prepared for:
Hewlett Packard Enterprise

11445 Compaq Center Drive West
Houston, Texas 77070

Prepared by:

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

Table of Contents

LIST OF TABLES

1. Security Target Introduction

This section introduces the Target of Evaluation (TOE) and provides the Security Target (ST) and TOE identification, ST and TOE conformance claims, ST conventions, glossary and list of abbreviations.

The TOE comprises the Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series, and MSR1000 Series routers, all with Comware V7.1. Each router is a stand-alone network appliance that provides layer 2 switching and layer 3 routing and service functions.

The Security Target contains the following additional sections:

- TOE Description (Section 2)—provides an overview of the TOE and describes the physical and logical boundaries of the TOE
- Security Problem Definition (Section 3)—describes the threats and assumptions that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the security objectives for the TOE and its operational environment necessary to counter the threats and satisfy the assumptions that define the security problem
- IT Security Requirements (Section 5)—specifies the security functional requirements (SFRs) and security assurance requirements (SARs) to be met by the TOE
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the SFRs
- Rationale (Section 7)—provides mappings and rationale for the security problem definition, security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series and MSR1000 Series Routers Security Target

ST Version – Version 1.0

ST Date – March 10, 2016

TOE Identification – Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series, and MSR1000 Series routers with Comware V7.1, as follows:

Product Series	Specific Devices	Comware Version
HP HSR6600	HP HSR6602-G Router (JG353A) HP HSR6602-XG Router (JG354A)	Comware 7.1.054, Release 7103 P05
HP HSR6800	HP HSR6802E Router Chassis (JG361B) HP HSR6804E Router Chassis (JG362B) HP HSR6808E Router Chassis (JG363B) Each of these devices requires an HP HSR6800 RSE-X3 Router Main Processing Unit (JH075A).	Comware 7.1.054, Release 7103 P05
HP MSR1000	HP MSR1003-8S AC Router (JH060A)	Comware 7.1.059, Release 0305

Table 1: TOE Series, Devices, and Comware Version

TOE Developer – Hewlett Packard Enterprise

Evaluation Sponsor – Hewlett Packard Enterprise

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012

1.2 Conformance Claims

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

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012
    - Part 3 Conformant

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

- EAL3 Augmented (ALC_FLR.2).

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (for example, [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (for example, [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (for example, [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (for example, "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Glossary

This ST uses a number of terms that have a specific meaning within the context of the ST and the TOE. This glossary provides a list of those terms and how they are to be understood within this ST.

CPOS	Channelized POS—uses low-speed tributary signals of STM-N to transmit multiple streams of data independent of one another over an optical fiber.
Dual-personality port	A dual-personality port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or an open mini-GBIC slot (for use with mini-GBIC transceivers).
Mini-GBIC	Alternative name for the small form-factor pluggable transceiver (SFP).

POS	Packet over SONET/SDH (POS) is a communications protocol for transmitting packets in the form of the Point to Point Protocol over SDH or SONET. A primary application of POS is to support sending of IP packets across Wide Area Networks.
SONET/SDH	Synchronous Optical Networking/Synchronous Digital Hierarchy—standardized protocols that transfer multiple digital bit streams synchronously over optical fiber.
SFP	(Communications) Small form-factor pluggable, a compact, hot-pluggable transceiver used for both telecommunication and data communications applications.
XFP	(10 Gigabit Small Form Factor Pluggable) a standard for transceivers for high-speed computer network and telecommunication links that use optical fiber.

1.5 Abbreviations and Acronyms

The following abbreviations and acronyms are used in this document. A brief definition is provided for abbreviations that are potentially unfamiliar, are specific to the TOE, or not obviously self-explanatory.

6PE	IPv6 to Provider Edge router
6vPE	IPv6 on VPN to Provider Edge router
ACL	Access Control List
AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CBC	Cipher-Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CM	Configuration Management
CLI	Command Line Interface
CPOS	Channelized POS
CPU	Central Processing Unit
DH	Diffie-Hellman
DSIC	Double-width SIC
EAL	Evaluation Assurance Level
EVB	Edge Virtual Bridging
FIPS	Federal Information Processing Standard
GbE	Gigabit Ethernet
GBIC	GigaBit Interface Converter—a standard for transceivers
GRE	Generic Routing Encapsulation
HIM	Hardware Interface Module
HMAC	Hashed Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers—professional association and standards body
IP	Internet Protocol
IPv4	Internet Protocol version 4
Ipv6	Internet Protocol version 6
IPsec	Internet Protocol Security
IRF	Intelligent Resilient Fabric
IS-IS	Intermediate System to Intermediate System
ISSU	In Service Software Upgrades
IT	Information Technology
LAN	Local Area Network
LDP	Label Distribution Protocol
MBGP	Multiprotocol BGP
MIM	Multifunction Interface Module
MPLS	Multiprotocol Label Switching
MPU	Main Processing Unit
Mpps	Millions of packets per second
MSDP	Multicast Source Discovery Protocol

NAT	Network Address Translation
NTP	Network Time Protocol
OAA	Open Application Architecture
OC	Optical Carrier
OSP	Organization Security Policy
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
POS	Packet over SONET/SDH (see glossary above)
PP	Protection Profile
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
RPR	Resilient Packet Ring—protocol for optimized data transport over optical fiber ring networks
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
RTC	Real Time Clock
RU	Rack Unit
SA	Security Association
SAP	Service Aggregation Platform
SAR	Security Assurance Requirement
SDH	Synchronous Digital Hierarchy
SFP	Security Function Policy
SFP	Small Form-factor Pluggable (see glossary above)
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SIC	Smart Interface Card
SIP	Session Initiation Protocol
SM	Security Management
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SSH	Secure Shell
ST	Security Target
STM-1	Synchronous Transport Module level-1—fiber optic network transmission standard
TACACS+	Terminal Access Controller Access Control System Plus
Tbps	Terabit per second
TCP	Transmission Control Protocol
TE	Traffic Engineering
TOE	Target of Evaluation
TRILL	Transparent Interconnection of Lots of Links
TSF	TOE Security Functions
VLAN	Virtual Local Area Network
VOQ	Virtual Output Queue
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
WAN	Wide Area Network

2. TOE Description

The Target of Evaluation (TOE) is the Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series, and MSR1000 Series routers, all with Comware V7.1.

The HSR6600 Series in the evaluated configuration consists of the following specific devices:

- HP HSR6602-G Router
- HP HSR6602-XG Router.

The HSR6800 Series in the evaluated configuration consists of the following specific devices:

- HP HSR6802E Router Chassis
- HP HSR6804E Router Chassis
- HP HSR6808E Router Chassis.

Each of these devices requires an HP HSR6800 RSE-X3 Router Main Processing Unit.

The MSR1000 Series in the evaluated configuration consists of the following specific device:

- HP MSR1003-8S AC Router.

Each series of routers comprising the TOE consists of a set of distinct devices (as identified in Section 1.1) that differ primarily according to power delivery, performance, and port density. Each device satisfies all of the security functional requirements specified in this ST.

2.1 TOE Overview

The various routers comprising the TOE are all Gigabit Ethernet router appliances that consist of hardware and software components. While the physical form factor of each of the three series of routers is substantially different, the underlying hardware shares a similar architecture. The software uses a common code base of a modular nature with only the modules applicable for the specific hardware installed.

This section identifies and describes the individual included devices in the TOE. The scope of the evaluation is the security functions specified in Section 6 (TOE Summary Specification) of this ST. Additional product features that are not within the scope of evaluation are described in order to provide information on the intended use of each device.

2.1.1 HSR6600 Series Routers

The HP HSR6600 Series are high-performance services WAN routers, designed for small-to-medium campus WAN edge and aggregation, and high-end branch, deployments. These routers are built with a compact multi-core centralized processing architecture that delivers, in a 2 RU form factor, routing, security, full layer 2 switching, and modular WAN and LAN interface options, all integrated in a single routing platform.

The HSR6602-G router has 4 dual-personality 1000 Mbps ports and 1 payload slot that can accommodate up to 4 modular interface cards.

The HSR6602-XG router, in addition to its 4 dual-personality 1000 Mbps ports and single payload slot, has 2 SPF+ 10GbE ports.

The following modules are supported by this series. They do not affect any of the claimed security functions and can be used to extend available network connectivity:

- HP 6600 8-port 10/100Base-T HIM Module (JC575A)
- HP 6600 4-port Gig-T HIM Module (JC163A)
- HP 6600 8-port Gig-T HIM Module (JC164A)
- HP 6600 4-port GbE SFP HIM Module (JC171A)
- HP 6600 8-port GbE SFP HIM Module (JC174A)

- HP 6600 1-port 10-GbE XFP HIM Module (JC168A)
- HP 6600 1-port OC-3/STM-1 (E1/T1) CPOS SFP HIM Module (JC161A)
- HP 6600 2-port OC-3/STM-1 (E1/T1) CPOS SFP HIM Module (JC162A)
- HP 6600 4-port OC-3c/STM-1c or 2-port OC-12c/STM-4c POS SFP HIM Module (JC172A)
- HP 6600 2-port OC-3c/STM-1c or 1-port OC-12c/STM-4c POS SFP HIM Module (JC173A)
- HP 6600 1-port OC-48c/STM-16c POS/CPOS SFP HIM Module (JC494A)
- HP 6600 8-port OC-3c/OC-12c POS/GbE SFP HIM Module (JG673A)
- HP MSR 2-port Enhanced Sync/Async Serial MIM Module (JD540A)
- HP MSR 8-port T1/Fractional T1 MIM Module (JC159A)
- HP MSR 8-port T1/CT1/PRI MIM Module (JC160A)
- HP MSR 4-port Enhanced Sync/Async Serial MIM Module (JD541A)
- HP MSR 8-port Enhanced Sync/Async Serial MIM Module (JD552A)
- HP 6600 FIP-20 Flexible Interface Platform Router Module (JG358A)

2.1.2 HSR6800 Series Routers

The HP HSR6800 Series are high-performance, multiservice router chassis designed for data center interconnection, enterprise WAN core, campus WAN edge, and high-speed WAN aggregation services. These devices feature a hardware architecture with multi-core CPUs and fully distributed routing and service engines for increased performance. All engines have separate control and service planes to avoid interference and to facilitate service continuity during an active/standby switchover. The distributed design allows packet forwarding and complicated services such as NAT, GRE, NetStream, QoS, and IPsec to be processed on each line card independently, thus enhancing the service processing performance of the overall system as line cards are added.

The switching fabric connects to the line cards through high-speed passive backplane channels and uses patent distributed scheduling algorithms and virtual output queues (VOQ) to perform inter-card forwarding, implementing non-blocking forwarding and end-to-end traffic control.

The devices in this series deliver routing, multicast, MPLS, IPv6, security, quality of service, carrier-level high-availability features, and high-density 10GbE and 1GbE interface options. They support all IPv4 and IPv6 routing protocols including RIP/RIPng, OSPF/OSPFv3, IS-IS/IS-ISv6, BGP/BGP4+, PIM/PIM6, MSDP, MBGP and policy-based routing, delivering increased flexibility. In addition, the series supports comprehensive MPLS features, including LDP, MPLS TE, L3 VPN, L2 VPN, VPLS, Multicast VPN, 6PE, and 6vPE, providing further flexibility.

The HP HSR6802E Router Chassis is a 5RU high-performance distributed architecture router platform that supports 2 MPUs in 1+1 redundancy and up to 2 service line cards. It provides up to 1.024 Tbps backplane bandwidth and 120 Mpps throughput via 2 SAP slots or 4 HIM slots or 8 MIM slots, or a combination thereof.

The HP HSR6804E Router Chassis is a 7RU high-performance distributed architecture router platform that supports 2 MPUs in 1+1 redundancy and up to 4 service line cards. It provides up to 1.024 Tbps backplane bandwidth and 240 Mpps throughput via 4 SAP slots or 8 HIM slots or 16 MIM slots, or a combination thereof.

The HP HSR6808E Router Chassis is a 20RU high-performance distributed architecture router platform that supports 2 MPUs in 1+1 redundancy and up to 8 service line cards. It provides up to 2.048 Tbps backplane bandwidth and 420 Mpps throughput via 8 SAP slots or 16 HIM slots or 32 MIM slots, or a combination thereof.

Each of the HSR6800 Series devices requires an HP HSR6800 RSE-X3 Router Main Processing Unit (MPU). The MPU supports the administrative interface for managing the chassis itself as well as the other networking modules installed in the chassis (see list of supported modules below). The MPU provides the following external interfaces:

- Management Ethernet port—a 10Base-T/100Base-TX/1000Base-T autosensing RJ-45 port that allows an administrator to manage the router through a network management server without using any service interface of the router. The management Ethernet port is used only for managing the router and has no service processing capabilities such as data forwarding.
- Console port—RS-232 asynchronous serial port that can be connected to a computer for system debugging, configuration, maintenance, management, and host software loading. It provides local access to the CLI.
- AUX port—RS-232 asynchronous serial port intended as a backup port if the local console port fails.

The HP HSR6800 Series uses Intelligent Resilient Fabric (IRF) to implement system virtualization. IRF enables two HSR6800 Routers to form and work as a single virtual device.

The following modules are supported by this series. They do not affect any of the claimed security functions and can be used to extend available network connectivity:

- HP 6600 8-port 10/100Base-T HIM Module (JC575A)
- HP 6600 4-port Gig-T HIM Module (JC163A)
- HP 6600 8-port Gig-T HIM Module (JC164A)
- HP 6600 4-port GbE SFP HIM Module (JC171A)
- HP 6600 8-port GbE SFP HIM Module (JC174A)
- HP 6600 1-port 10-GbE XFP HIM Module (JC168A)
- HP 6600 1-port OC-3/STM-1 (E1/T1) CPOS SFP HIM Module (JC161A)
- HP 6600 2-port OC-3/STM-1 (E1/T1) CPOS SFP HIM Module (JC162A)
- HP 6600 4-port OC-3c/STM-1c or 2-port OC-12c/STM-4c POS SFP HIM Module (JC172A)
- HP 6600 2-port OC-3c/STM-1c or 1-port OC-12c/STM-4c POS SFP HIM Module (JC173A)
- HP 6600 1-port OC-48c/STM-16c POS/CPOS SFP HIM Module (JC494A)
- HP MSR 2-port Enhanced Sync/Async Serial MIM Module (JD540A)
- HP MSR 8-port T1/Fractional T1 MIM Module (JC159A)
- HP MSR 8-port T1/CT1/PRI MIM Module (JC160A)
- HP MSR 4-port Enhanced Sync/Async Serial MIM Module (JD541A)
- HP MSR 8-port Enhanced Sync/Async Serial MIM Module (JD552A)
- HP 6600 8-port OC-3c/OC-12c POS/GbE SFP HIM Module (JG673A)
- HP 8-port E1/CE1/PRI (75ohm) MIM Router (RT-MIM-8E1(75)-H3) A-MSR Module (JD563A)
- HP HSR6800 4-port 10GbE SFP+ Service Aggregation Platform Router Module (JG366A)
- HP HSR6800 FIP-300 Flexible Interface Platform Module (JG671A)
- HP HSR6800 FIP-310 Flexible Interface Platform Module (JG672A)
- HP HSR6800 FIP-600 Flexible Interface Platform Router Module (JG360A)
- HP HSR6808 SFE-X1 Switch Fabric Engine Router Module (JG365A)
- HP 6600 FIP-240 Flexible Interface Platform Module (JH137A)
- HP 6600 16-port GbE SFP and 12-port Combo GbE Service Aggregation Platform Module (JH138A)
- HP 6600 16-port GbE SFP 4-port GbE Combo and 2-port 10GbE SFP+ Service Aggregation Platform Module (JH139A)

2.1.3 MSR1000 Series Routers

The HP MSR1000 Series are high-performance, entry-level, small branch routers that deliver integrated routing, switching, security, mobility, and SIP in a single box. With an integrated infrastructure and modular design, the MSR1000 Series reduces complexity and simplifies the network through integrated routing/ switching/ security/ voice/ 3G and 4G LTE WAN.

The MSR1003-8S AC router provides 3 SIC or 1 SIC and 1 DSIC module slots, 2 RJ-45 autosensing 10/100/1000 WAN ports, and 8 RJ-45 autosensing 10/100/1000 LAN ports, supporting up to 500Kpps forwarding and 170Mbps of IPsec encryption throughput.

The following modules are supported by this series. They do not affect any of the claimed security functions and can be used to extend available network connectivity:

- HP MSR 9-port 10/100Base-T Switch DSIC Module (JD574B)
- HP MSR 4-port 10/100Base-T Switch SIC Module (JD573B)
- HP MSR 4-port Gig-T Switch SIC Module (JG739A)
- HP MSR 1-port GbE Combo SIC Module (JG738A)
- HP MSR 1-port 10/100Base-T SIC Module (JD545B)
- HP MSR 1-port 100Base-X SIC Module (JF280A)
- HP MSR 2-port FXO SIC Module (JD558A)
- HP MSR 2-port FXS SIC Module (JD560A)

- HP MSR 2-port FXS/1-port FXO SIC Module (JD632A)
- HP MSR 2-port ISDN-S/T Voice SIC Module (JF821A)
- HP MSR 1-port ADSL2+ SIC Module (JD537A)
- HP MSR 1-port ADSL over ISDN SIC Module (JG056B)
- HP MSR 1-port 8-wire G.SHDSL (RJ45) DSIC Module (JG191A)
- HP MSR 1-port E1/Fractional E1 (75ohm) SIC Module (JD634B)
- HP MSR 2-port E1/Fractional E1 (75ohm) SIC Module (JF842A)
- HP MSR 1-port T1/Fractional T1 SIC Module (JD538A)
- HP MSR 1-port Enhanced Serial SIC Module (JD557A)
- HP MSR 2-port Enhanced Sync / Async Serial SIC Module (JG736A)
- HP MSR 4-port Enhanced Sync / Async Serial SIC Module (JG737A)
- HP MSR 1-port ISDN-S/T SIC Module (JD571A)
- HP MSR 16-port Async Serial SIC Module (JG186A)
- HP MSR 8-port Async Serial SIC Module (JF281A)
- HP MSR 1-port E1/CE1/PRI SIC Module (JG604A)
- HP MSR 4-port FXS / 1-port FXO DSIC Module (JG189A)
- HP MSR HSPA/WCDMA SIC Module (JG187A)
- HP MSR 4G LTE SIC Module for Verizon/LTE 700 MHz/CDMA Rev A (JG742A)
- HP MSR 4G LTE SIC Module for ATT/LTE 700/1700/2100 MHz and UMTS/HSPA+/HSPA/EDGE/GRPS/GSM (JG743A)
- HP MSR 4G LTE SIC Module for Global/LTE 800/900/1800/2100/2600 MHz and UMTS/HSPA+/HSPA/EDGE/GRPS/GSM (JG744A)
- HP MSR HSPA+ / WCDMA SIC Module (JG929A)

2.2 TOE Architecture

The various routers comprising the TOE share a common software code base, called Comware. Comware is special purpose appliance system software that implements a wide array of networking technology, including: IPv4/IPv6 dual-stacks; a data link layer; layer 2 and 3 routing; Ethernet switching; Virtual Local Area Networks (VLANs); and Quality of Service (QoS). The evaluated version of Comware is V7.1. It should be noted that Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows, but the only underlying architecture found in the evaluated configuration is Linux.

Comware V7.1 implements full modularization and multi-process applications, providing the following benefits:

- Full modularization brings improvements in system availability, virtualization, multi-core multi-CPU applications, distributed computing, and dynamic loading and upgrading.
- Openness—Comware V7.1 is a generic, open system based on Linux
- Improved operations—Comware V7.1 improves some detailed operations. For example, it uses preemptive scheduling to improve real-time performance.

Comware V7.1 optimizes the following functions:

- Virtualization—Supports N:1 virtualization.
- ISSU—Supports ISSU for line cards.
- Auxiliary CPU and OAA—Improve scalability for devices.

In addition, Comware V7.1 supports new technologies for data centers, including Transparent Interconnection of Lots of Links (TRILL), and Edge Virtual Bridging (EVB).

Comware V7.1 comprises the following four planes, as depicted in Figure 1 below:

- Infrastructure plane—provides basic Linux services and Comware support functions. Basic Linux services comprise basic Linux functions, C language library functions, data structure operations, and standard algorithms. Comware support functions provide software and service infrastructures for Comware processes, including all basic functions.

- Data plane—provides data forwarding for local packets and received IPv4 and IPv6 packets at different layers.
- Control plane—comprises all routing, signaling, and control protocols, such as MPLS, OSPF, and security control protocols. It generates forwarding tables for the data plane.
- Management plane—provides a management interface for operators to configure, monitor, and manage Comware V7.1. The management interface comprises a command line interface (CLI) accessed using Secure Shell (SSH).

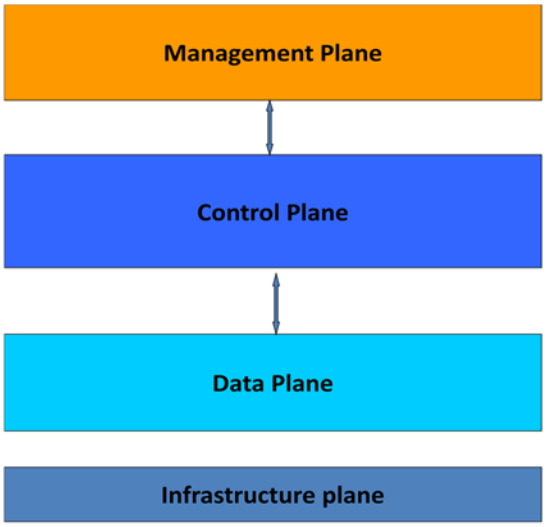

Figure 1: Comware V7.1 Architecture

2.2.1 Physical Boundaries

A device in the HSR6600 Router Series or MSR1000 Router Series is a physical network appliance with a fixed number of ports, while a device in the HSR6800 Router Series is a physical network appliance chassis supporting a fixed number of service line cards. The specific devices in each series are identified in Section 1.1. Each series also supports a variety of modules that provide a wide range of network ports varying in number, form factor (copper or fiber), and performance (1 – 10 Gb). The applicable modules for each series are identified in Section 2.1.

In its evaluated configuration, the TOE can make use of the following external IT entities in its operational environment[1]:

- Syslog server—the TOE can be configured to export generated audit records to an external syslog server.
- RADIUS and TACACS+ servers—the TOE can be configured to use external authentication servers.
- NTP server—the TOE can be configured to use the Network Time Protocol to keep the local hardware-based real-time clock synchronized with other network devices.
- Management workstation—the TOE supports remote administrative access to its command line interface (CLI) via Secure Shell (SSH), the use of which requires SSHv2 client software.

2.2.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit
- Cryptographic support

[1] The TOE also supports SNMPv3, but use of this protocol to connect to the TOE is excluded from the evaluated configuration.

- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels.

2.2.2.1 Security Audit

The TOE is able to generate audit records of security-relevant events occurring on the TOE. Generated audit records include a date and time stamp, the nature or type of the triggering event, an indication of the event outcome, and identification of the agent responsible for the event. The TOE provides administrators with the ability to review audit records stored in the audit trail. The audit records are stored on the TOE appliance, where they are protected from unauthorized modification and deletion. The TOE can also be configured to export audit records to an external audit server.

2.2.2.2 Cryptographic Support

The TOE implements cryptographic algorithms that provide key management, random bit generation, data encryption and decryption, digital signature generation and verification, and secure hashing and key-hashing features in support of higher level cryptographic protocols, including IPsec and SSHv2. Note that in the evaluated configuration, the TOE must be configured in FIPS mode, which ensures the TOE's configuration is consistent with the FIPS 140-2 standard.

2.2.2.3 User Data Protection

The TOE provides firewall capabilities that allow for the definition of firewall rules, collectively known as access control lists (ACLs), which are applied to applicable network traffic as it is received and which would pass through the TOE between connected networks. The ACLs can be basic, with matching criteria based only on source IP address, or advanced, with matching criteria based on source and destination addresses, transport layer protocol, and service. ACLs can also be defined independently for both IPv4 and IPv6 network traffic and can be assigned to specific TOE interfaces.

2.2.2.4 Identification and Authentication

The TOE requires administrators to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers a locally connected console and a network-accessible interface (via SSHv2) for interactive administrator sessions.

The TOE supports the local (that is, on device) definition of administrators with usernames and passwords. Additionally, the TOE can be configured to utilize the services of trusted RADIUS and TACACS+ servers in the operational environment to support, for example, centralized user administration.

2.2.2.5 Security Management

The TOE provides a CLI to access its security management functions. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE.

2.2.2.6 Protection of the TSF

The TOE implements a number of self-tests that it performs when it starts up, to ensure its cryptographic functions operate properly and that the Comware and TSF executable files have not been modified.

The TOE includes its own time source for providing reliable time stamps that are used in audit records.

2.2.2.7 TOE Access

The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator.

The TOE allows administrators to terminate their own interactive sessions.

2.2.2.8 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access. Using SSHv2, both integrity and disclosure protection is ensured.

The TOE can be configured to use IPsec to protect communications with external IT entities, such as audit and authentication servers, against disclosure or undetected modification of data.

2.3 TOE Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, there are four Common Criteria specific guides that reference the security-related guidance material for all products covered in the scope of evaluation:

- *Preparative Procedures for CC EAL3 Evaluated Hewlett Packard Enterprise HSR6800, HSR6600 and MSR1000 router series based on Comware V7.1*, Version 1.01, dated 2016-01-04
- *Command Reference for CC Supplement*, Revision 1.05, dated 2015-12-02
- *Configuration Guide for CC Supplement*, Revision 1.6, dated 2015-12-02
- *Comware V7 Platform System Log Messages*, Revision 1.00, dated 2015-12-02.

The links in Appendix A for each series can be used to find the full set of documentation for each of the evaluated router series. The following documents (available for each series) were specifically examined during the evaluation.

- *Security Configuration Guide*
- *Security Command Reference*
- *Fundamentals Configuration Guide*
- *Fundamentals Command Reference*
- *Network Management and Monitoring Configuration Guide*
- *Network Management and Monitoring Command Reference*
- *ACL and QoS Configuration Guide*
- *ACL and QoS Command Reference*
- *Layer-3 IP Services Configuration Guide*
- *Layer-3 IP Services Command Reference*
- *Installation Guide*

3. Security Problem Definition

This section defines the security problem to be addressed by the TOE, in terms of threats to be countered by the TOE or its operational environment, and assumptions about the intended operational environment of the TOE.

3.1 Assumptions

This section contains assumptions regarding the operational environment and the intended usage of the TOE.

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

3.2 Threats

This section identifies and describes the threats to be countered by the TOE and its operational environment.

T.BRUTE_FORCE	An unauthorized user may gain access to the TOE through repeated password-guessing attempts.
T.MEDIATE	An unauthorized IT entity may send information through the TOE to compromise IT entities on an internal (protected) network.
T.NETWORK_COMPROMISE	TSF data communicated between the TOE and external entities is disclosed or undetectably modified.
T.NO_ACCOUNTABILITY	Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.
T.UNATTENDED_SESSION	An unauthorized user gains access to the TOE via an unattended authorized user session.
T.UNAUTHORIZED_ACCESS	Unauthorized users gain access to the TOE and its services.
T.UNAUTHORIZED_ACTIVITY	Authorized users perform unauthorized actions on the TOE.

4. Security Objectives

This section identifies the security objectives for the TOE and its operational environment. The security objectives identify the responsibilities of the TOE and its environment in addressing the security problem defined in Section 3.

4.1 Security Objectives for the TOE

The following are the TOE security objectives:

O.AUDIT	The TOE shall be able to generate audit records of security-relevant events, identifying users causing the events as applicable.
O.AUDIT_REVIEW	The TOE shall provide a means for authorized users to review the audit records generated by the TOE.
O.AUDIT_STORAGE	The TOE shall protect stored audit records from unauthorized modification and deletion and shall provide a means to prevent the loss of audit records in the event the space available for storing them is exhausted.
O.CRYPTOGRAPHY	The TOE shall perform cryptographic operations to support protocols used to protect data in transit.
O.I_&_A	The TOE shall require all users of the TOE to be identified and authenticated before gaining access to TOE services.
O.MEDIATE	The TOE shall mediate the flow of information from IT entities on one connected network to IT entities on another connected network.
O.PASSWORD_CONTROLS	The TOE shall provide a mechanism to reduce the likelihood that users choose weak passwords.
O.PROTECTED _COMMS	The TOE shall protect communications between the TOE and external entities from disclosure and undetected modification.
O.SECURITY_MANAGEMENT	The TOE shall restrict the ability to perform security management functions on the TOE to authorized administrators having appropriate privileges.
O.SESSION_TERMINATION	The TOE shall provide mechanisms to terminate a user session after a period of inactivity or at the request of the user.
O.THROTTLE	The TOE shall limit the rate at which consecutive unsuccessful authentication attempts can be performed.

4.2 Security Objectives for the Operational Environment

The following are the security objectives for the operational environment of the TOE:

OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.PERSONNEL	Those responsible for the TOE must ensure that personnel working as authorized administrators have been carefully selected and trained for proper operation of the TOE.

5. IT Security Requirements

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. SFRs were drawn exclusively from Part 2 of the Common Criteria v3.1 Revision 4.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_SAR.3: Selectable audit review
	FAU_STG.1: Protected audit trail storage
	FAU_STG.4: Prevention of audit data loss
FCS: Cryptographic support	FCS_CKM.1: Cryptographic key generation
	FCS_CKM.4: Cryptographic key destruction
	FCS_COP.1(1): Cryptographic operation (encryption/decryption)
	FCS_COP.1(2): Cryptographic operation (digital signature)
	FCS_COP.1(3): Cryptographic operation (cryptographic hashing)
	FCS_COP.1(4): Cryptographic operation (keyed-hash)
	FCS_COP.1(5): Cryptographic operation (random number generation)
FDP: User data protection	FDP_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
FIA: Identification and authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	FIA_SOS.1: Verification of secrets
	FIA_UAU.2: User authentication before any action
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UAU.7: Protected authentication feedback
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MOF.1: Management of security functions behaviour
	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialisation
	FMT_MTD.1: Management of TSF Data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles

Requirement Class	Requirement Component
FPT: Protection of the TSF	FPT_STM.1: Reliable time stamps
	FPT_TST.1: TSF testing
FTA: TOE access	FTA_SSL.3: TSF-initiated termination
	FTA_SSL.4: User-initiated termination
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1: Trusted path

Table 2: TOE Security Functional Components

5.1.1 Security Audit (FAU)

FAU_GEN.1 – Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [***not specified***] level of audit; and
c) [**The events listed in Table 3**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**information specified in Table 3**].

Requirement	Auditable Events	Additional Audit Record Contents
FDP_IFF.1	Decisions to permit requested information flows.	The presumed addresses of the source and destination subject.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by an administrator of the user's capability to authenticate.	The identity of the offending user and the administrator.
FIA_SOS.1	Rejection by the TSF of any tested secret.	No additional information.
FIA_UAU.2	Any use of the authentication mechanism.	The user identity provided to the TOE.
FIA_UAU.5	The final decision on authentication.	The user identity provided to the TOE.
FIA_UID.2	Any use of the identification mechanism.	The user identity provided to the TOE.
FMT_SMF.1	Use of the management functions.	The identity of the administrator performing the operation.
FMT_SMR.1	Modifications to the group of users that are part of an administrator role.	The identity of the administrator performing the modification and the user identity being associated with the administrator role
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address). The identity of the administrator performing the operation
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.

Requirement	Auditable Events	Additional Audit Record Contents
FTP_ITC.1	Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channel functions.
FTP_TRP.1	Failures of the trusted path functions.	Identification of the user associated with all trusted path failures, if available.

Table 3: Auditable Events

FAU_GEN.2 – User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 – Audit review

FAU_SAR.1.1 The TSF shall provide [**Network Administrator, Network Operator**] with the capability to read [**all audit trail data**] from the audit records.

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

FAU_SAR.3 – Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**searches**] of audit data based on [
a) presumed subject address;
b) ranges of dates;
c) ranges of times; and/or
d) ranges of addresses].

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.

FAU_STG.4 – Prevention of audit data loss

FAU_STG.4.1 The TSF shall [***overwrite the oldest stored audit records***] and [**send generated audit records to a configured external syslog server**] if the audit trail is full.

5.1.2 Cryptographic Support (FCS)

FCS_CKM.1 – Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA key generation**] and specified cryptographic key sizes [**2048 bits**] that meet the following: [**FIPS 186-4**].

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 [**key zeroization**] that meets the following: [**FIPS 140-2**].

FCS_COP.1(1) – Cryptographic operation (encryption/decryption)

FCS_COP.1.1(1) The TSF shall perform [**symmetric encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in CBC mode**] and cryptographic key sizes [**128, 192, 256 bits**] that meet the following: [**FIPS 197**].

FCS_COP.1(2) – Cryptographic operation (digital signature)

FCS_COP.1.1(2) The TSF shall perform [**digital signature generation and verification**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**2048 bits**] that meet the following: [**FIPS 186-4**].

FCS_COP.1(3) – Cryptographic operation (cryptographic hashing)

FCS_COP.1.1(3) The TSF shall perform [**cryptographic hashing**] in accordance with a specified cryptographic algorithm [**SHA-1, SHA-256, SHA-512**] and cryptographic ~~key~~ **hash** sizes [**160, 256, 512 bits**] that meet the following: [**FIPS 180-3**].

FCS_COP.1(4) – Cryptographic operation (keyed-hash)

FCS_COP.1.1(4) The TSF shall perform [**keyed-hash message authentication**] in accordance with a specified cryptographic algorithm [**HMAC-SHA-1**] and cryptographic key sizes [**Key Size ≤ 512 bits**] that meet the following: [**FIPS 198-1, FIPS 180-3**].

FCS_COP.1(5) – Cryptographic operation (random number generation)

FCS_COP.1.1(5) The TSF shall perform [**random number generation**] in accordance with a specified cryptographic algorithm [**ANSI X9.31 Appendix A.2.4 Using AES on HSR6600/6800; CTR_DRBG (AES) on MSR1000**] and cryptographic key sizes [**128 bits**] that meet the following: [**FIPS 140-2 Annex C for ANSI X9.31; NIST Special Publication 800-90 for CTR_DRBG (AES)**].

5.1.3 User Data Protection (FDP)

FDP_IFC.1 – Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [**UNAUTHENTICATED SFP**] on [
a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;
b) information: traffic sent through the TOE from one subject to another;
c) operation: pass information].

FDP_IFF.1 – Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [**UNAUTHENTICATED SFP**] based on at least the following types of subject and information security attributes: [
a) subject security attributes:
- **presumed address;**

b) information security attributes (IPv4 or IPv6):
- **presumed address of source subject;**
- **presumed address of destination subject;**
- **transport layer protocol;**
- **other header fields (ack, fin, psh, rst, syn, urg);**
- **ICMP type;**
- **source and destination ports;**
- **time stamp;**
- **TOE interface on which traffic arrives and departs].**

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

- **the presumed address of the source subject, in the information, 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 Network 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 The TSF shall enforce the [**no additional information flow control SFP rules**].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [**no additional rules, based on security attributes that explicitly authorize information flows**].

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

a) [**No additional rules.**]

5.1.4 Identification and Authentication (FIA)

FIA_AFL.1 – Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within [positive integers greater than 0]***] of unsuccessful authentication attempts occur related to [**login**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**terminate the session establishment process and lock user account until manually unlocked by an administrator or the configured locking period has expired**].

FIA_ATD.1 – User attribute definition

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

- **Identity**
- **Authentication data**
- **Role**].

FIA_SOS.1 – Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**the following rules:**

- **each locally defined user password must be a minimum of 15 characters in length;**
- **each locally defined user password must be composed of at least one each of: lower case alphabetic characters, upper case alphabetic characters, numbers, and special characters**].

FIA_UAU.2 – User authentication before any action

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

FIA_UAU.5 – Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [**password and RSA certificate (public-key) mechanisms and support for remote RADIUS and TACACS+ services**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**following rules:**

- **SSH authentication can be configured on the TOE on a per-user basis to require a password, or both a password and RSA certificate**

- **SSH and console authentication utilize only those authentication mechanisms configured by a Network Administrator**
- **SSH and console authentication check the configured authentication mechanisms in the order they are configured by a Network Administrator**].

FIA_UAU.7 – Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only [**obscured feedback**] to the user while the authentication is in progress.

FIA_UID.2 – User identification before any action

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

5.1.5 Security Management (FMT)

FMT_MOF.1 – Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable***, ***enable***, ***modify the behaviour of***] the functions [**remote authentication**] to [**a Network Administrator**].

FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**UNAUTHENTICATED SFP**] to restrict the ability to [***modify***, ***delete***, ***[create]***] the security attributes [**information flow security policy rules**] to [**a Network Administrator**].

FMT_MSA.3 – Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [**UNAUTHENTICATED 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 [**Network Administrator**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(1) – Management of TSF data (audit trail)

FMT_MTD.1.1(1) The TSF shall restrict the ability to [***clear***, ***[archive]***] the [**audit trail**] to [**the Network Administrator**].

FMT_MTD.1(2) – Management of TSF data (user accounts)

FMT_MTD.1.1(2) The TSF shall restrict the ability to [***modify***, ***delete***, ***[create, restore]***] the [**user accounts**] to [**the Network Administrator**].

FMT_MTD.1(3) – Management of TSF data (other security controls)

FMT_MTD.1.1(3) The TSF shall restrict the ability to [***modify***] the [**password controls, date/time settings**] to [**the Network Administrator**].

FMT_SMF.1 – Specification of Management Functions

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

- **Manage the audit trail**
- **Manage firewall rules**
- **Manage user accounts**
- **Manage password controls**
- **Manage date/time settings**
- **Manage remote authentication capabilities**].

FMT_SMR.1 – Security management roles

FMT_SMR.1.1 The TSF shall maintain the roles [**Network Administrator, Network Operator**].

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

Application Note: 'Network Administrator' is realized in the TOE by the network-admin role, while 'Network Operator' is realized by the network-operator role. The TOE supports additional security management roles, but these do not have any specific capabilities related to the security management or other functional requirements specified in the ST.

5.1.6 Protection of the TSF (FPT)

FPT_STM.1 – Reliable time stamps

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

FPT_TST.1 – TSF testing

FPT_TST.1.1 The TSF shall run a suite of self-tests [***during initial start-up***] to demonstrate the correct operation of [***[TOE cryptographic module]***].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [***[Comware executable file]***].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [***[stored TSF executable code]***].

5.1.7 TOE Access (FTA)

FTA_SSL.3 – TSF-initiated termination

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

FTA_SSL.4 – User-initiated termination

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

5.1.8 Trusted Path/Channels (FTP)

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***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**sending audit records to a remote syslog server**].

FTP_TRP.1 –Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***disclosure, [undetected modification]***].

FTP_TRP.1.2 The TSF shall permit [***remote users***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***initial user authentication, [remote administration functions]***].

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL3 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.3: Functional specification with complete summary
	ADV_TDS.2: Architectural design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.3: Authorisation controls
	ALC_CMS.3: Implementation representation CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_DVS.1: Identification of security measures
	ALC_FLR.2: Flaw reporting procedures
	ALC_LCD.1: Developer defined life-cycle model
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.2: Analysis of coverage
	ATE_DPT.1: Testing: basic design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 4: EAL3 Assurance Components

5.2.1 Development (ADV)

ADV_ARC.1 – Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C	The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
ADV_ARC.1.3C	The security architecture description shall describe how the TSF initialisation process is secure.
ADV_ARC.1.4C	The security architecture description shall demonstrate that the TSF protects itself from tampering.
ADV_ARC.1.5C	The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.
ADV_ARC.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.3 – Functional specification with complete summary

ADV_FSP.3.1D	The developer shall provide a functional specification.
ADV_FSP.3.2D	The developer shall provide a tracing from the functional specification to the SFRs.
ADV_FSP.3.1C	The functional specification shall completely represent the TSF.
ADV_FSP.3.2C	The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.3.3C	The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.3.4C	For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
ADV_FSP.3.5C	For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from SFR-enforcing actions and exceptions associated with invocation of the TSFI.
ADV_FSP.3.6C	The functional specification shall summarise the SFR-supporting and SFR-non-interfering actions associated with each TSFI.
ADV_FSP.3.7C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.3.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.2 – Architectural design

ADV_TDS.2.1D	The developer shall provide the design of the TOE.
ADV_TDS.2.2D	The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
ADV_TDS.2.1C	The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.2.2C	The design shall identify all subsystems of the TSF.
ADV_TDS.2.3C	The design shall describe the behavior of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR-non-interfering.
ADV_TDS.2.4C	The design shall describe the SFR-enforcing behavior of the SFR-enforcing subsystems.
ADV_TDS.2.5C	The design shall summarise the SFR-supporting and SFR-non-interfering behaviour of the SFR-enforcing subsystems.
ADV_TDS.2.6C	The design shall summarise the behaviour of the SFR-supporting subsystems.
ADV_TDS.2.7C	The design shall provide a description of the interactions among all subsystems of the TOE.
ADV_TDS.2.8C	The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.
ADV_TDS.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.2.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance Documents (AGD)

AGD_OPE.1 – Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 – Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle Support (ALC)

ALC_CMC.3 – Authorisation controls

ALC_CMC.3.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.3.2D The developer shall provide the CM documentation.

ALC_CMC.3.3D The developer shall use a CM system.

ALC_CMC.3.1C The TOE shall be labelled with its unique reference.

ALC_CMC.3.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.3.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.3.4C	The CM system shall provide measures such that only authorised changes are made to the configuration items.
ALC_CMC.3.5C	The CM documentation shall include a CM plan.
ALC_CMC.3.6C	The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.3.7C	The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.3.8C	The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.
ALC_CMC.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.3 – Implementation representation CM coverage

ALC_CMS.3.1D	The developer shall provide a configuration list for the TOE.
ALC_CMS.3.1C	The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE; and the implementation representation.
ALC_CMS.3.2C	The configuration list shall uniquely identify the configuration items.
ALC_CMS.3.3C	For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 – Delivery procedures

ALC_DEL.1.1D	The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2D	The developer shall use the delivery procedures.
ALC_DEL.1.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1 – Identification of security measures

ALC_DVS.1.1D	The developer shall produce and provide development security documentation.
ALC_DVS.1.1C	The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2E	The evaluator shall confirm that the security measures are being applied.

ALC_FLR.2 – Flaw reporting procedures

ALC_FLR.2.1D	The developer shall document and provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2D	The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3D	The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.2.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5C	The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6C	The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
ALC_FLR.2.7C	The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8C	The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_LCD.1 – Developer defined life-cycle model

ALC_LCD.1.1D	The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.
ALC_LCD.1.2D	The developer shall provide life-cycle definition documentation.
ALC_LCD.1.1C	The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
ALC_LCD.1.2C	The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.
ALC_LCD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Security Target Evaluation (ASE)

ASE_CCL.1 – Conformance claims

ASE_CCL.1.1D	The developer shall provide a conformance claim.
ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C	The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 – Extended components definition

ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
ASE_ECD.1.2D	The developer shall provide an extended components definition.
ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C	The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C	The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C	The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_INT.1 – ST introduction

ASE_INT.1.1D	The developer shall provide an ST introduction.
ASE_INT.1.1C	The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
ASE_INT.1.2C	The ST reference shall uniquely identify the ST.
ASE_INT.1.3C	The TOE reference shall identify the TOE.
ASE_INT.1.4C	The TOE overview shall summarise the usage and major security features of the TOE.
ASE_INT.1.5C	The TOE overview shall identify the TOE type.
ASE_INT.1.6C	The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
ASE_INT.1.7C	The TOE description shall describe the physical scope of the TOE.
ASE_INT.1.8C	The TOE description shall describe the logical scope of the TOE.
ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_OBJ.2 – Security objectives

ASE_OBJ.2.1D	The developer shall provide a statement of security objectives.
ASE_OBJ.2.2D	The developer shall provide a security objectives rationale.
ASE_OBJ.2.1C	The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.
ASE_OBJ.2.2C	The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C	The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.
ASE_OBJ.2.4C	The security objectives rationale shall demonstrate that the security objectives counter all threats.
ASE_OBJ.2.5C	The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.
ASE_OBJ.2.6C	The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.
ASE_OBJ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_REQ.2 – Derived security requirements

ASE_REQ.2.1D	The developer shall provide a statement of security requirements.
ASE_REQ.2.2D	The developer shall provide a security requirements rationale.
ASE_REQ.2.1C	The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.2.2C	All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.2.3C	The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.2.4C	All operations shall be performed correctly.
ASE_REQ.2.5C	Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.2.6C	The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
ASE_REQ.2.7C	The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
ASE_REQ.2.8C	The security requirements rationale shall explain why the SARs were chosen.
ASE_REQ.2.9C	The statement of security requirements shall be internally consistent.
ASE_REQ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 – Security problem definition

ASE_SPD.1.1D	The developer shall provide a security problem definition.
ASE_SPD.1.1C	The security problem definition shall describe the threats.
ASE_SPD.1.2C	All threats shall be described in terms of a threat agent, an asset, and an adverse action.
ASE_SPD.1.3C	The security problem definition shall describe the OSPs.
ASE_SPD.1.4C	The security problem definition shall describe the assumptions about the operational environment of the TOE.
ASE_SPD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 – TOE summary specification

ASE_TSS.1.1D	The developer shall provide a TOE summary specification.
ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.5 Tests (ATE)

ATE_COV.2 – Analysis of coverage	
ATE_COV.2.1D	The developer shall provide an analysis of the test coverage.
ATE_COV.2.1C	The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.2.2C	The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.
ATE_COV.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 – Testing: basic design	
ATE_DPT.1.1D	The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1C	The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.
ATE_DPT.1.2C	The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.
ATE_DPT.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 – Functional testing	
ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
ATE_FUN.1.1C	The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C	The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 – Independent testing – sample	
ATE_IND.2.1D	The developer shall provide the TOE for testing.
ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6 Vulnerability Assessment (AVA)

AVA_VAN.2 – Vulnerability analysis	
AVA_VAN.2.1D	The developer shall provide the TOE for testing.
AVA_VAN.2.1C	The TOE shall be suitable for testing.

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

The TOE implements the following security functions that together satisfy the SFRs claimed in Section 5.1 of this ST:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels.

6.1 Security Audit

The TOE is able to generate audit records for security relevant and other events as they occur. The events that can cause an audit record to be generated include starting and stopping the audit function, as well as all of the events identified in Table 3.

The generated audit records include the date and time the record was generated, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome; and the identity of the agent responsible for the event (e.g., user name or network host IP address). The generated audit records also include event-specific content that includes the details specified in Table 3.

The TOE includes an internal log implementation that can be used to store and review audit records locally. The maximum storage space reserved for the local log file can be configured to a range between 1 and 10MB. When the local log storage is full, the TOE will overwrite the oldest records with new records. Users in the network-admin or network-operator role are able to view the contents of the local log file. The functions available to review audit records allow the audit records to be searched using regular expressions on the following audit record information: presumed subject address; range of dates; range of times; range of addresses. Users in the network-admin role additionally can delete (but not modify) or archive stored audit records using available CLI commands specifically designed for the management of the internal audit trail. Additionally, the TOE can be configured to send generated audit records to an external syslog server.

Note that the TOE can also be configured to create a subset of the log file, called `seclog.log`, which records security information such as logs of authentication and authorization events. A user in the security-audit role has exclusive access to `seclog.log`. However, `seclog.log` does not record all audit events as specified in Table 3, so cannot be regarded as the TOE audit trail.

The Security Audit function satisfies the following security functional requirements:

- FAU_GEN.1—the TOE can generate audit records for the security-relevant events identified in Table 3. Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in Table 3.
- FAU_GEN.2—the TOE identifies the responsible user for each event, based on the specific administrator or network entity (identified by IP address) that caused the event.
- FAU_SAR.1—the audit trail can be fully reviewed by users in the network-admin or network-operator role.
- FAU_SAR.3—the available log review tools support searching. Searching is based on any attributes or ranges thereof using regular expressions.

- FAU_STG.1—the TOE can be configured to export audit records to an external syslog server and can be configured to use IPsec for communication with the syslog server.
- FAU_STG.4—the TOE overwrites the oldest audit records in the internal audit trail with new audit records when the audit trail becomes full. The TOE can be configured to send audit records to an external syslog server as they are recorded.

6.2 Cryptographic Support

The TOE implements cryptographic algorithms providing supporting cryptographic functions. The following functions have been certified in accordance with the identified standards.

		Certificates	
Functions	**Standards**	**HSR6600/HSR6800**	**MSR1000**
Asymmetric key generation			
RSA key pair generation	FIPS 186-4	RSA #1968	RSA #1969
Encryption/Decryption			
AES in CBC mode (128, 192, 256 bits)	FIPS 197	AES #3853 AES #3851 (kernel)	AES #3855 AES #3854 (kernel)
Cryptographic signature services			
RSA Digital Signature Algorithm (modulus 2048 bits)	FIPS 186-4	RSA #1968	RSA #1969
Cryptographic hashing			
SHA-1, SHA-256, SHA-512 (digest sizes 160, 256 and 512 bits)	FIPS 180-3	SHA #3175 SHA #3173 (kernel)	SHA #3177 SHA #3176 (kernel)
Keyed-hash message authentication			
HMAC-SHA (key size ≤ 512 bits, digest size 160 bits)	FIPS 198-1 FIPS 180-3	HMAC #2501 HMAC #2499 (kernel)	HMAC #2503 HMAC #2502 (kernel)
Random number generation			
ANSI X9.31 App. A.2.4 using AES	FIPS 140-2 Annex C	RNG #1412	n/a
CTR_DRBG(AES)	NIST SP 800-90	n/a	DRBG #1094

Table 5: Cryptographic Services

The TOE includes a crypto-module providing supporting cryptographic functions.

The HSR6600 Series and HSR6800 Series devices within the TOE implement an ANSI X9.31 random number generator to generate keys to support AES CBC encryption. The MSR1000 Series devices implement a CTR_DRBG (AES) random bit generator for the same purpose. The AES implementation satisfies FIPS PUB 197.

The TOE supports SSHv2 with AES (CBC) 128 or 256 bit keys in conjunction with HMAC-SHA-1 or HMAC-SHA-1-96 and user authentication using RSA key pairs. The TOE implementation of HMAC-SHA-1 and HMAC-SHA-1-96 meets FIPS PUB 198-1 and FIPS PUB 180-3. The TOE generates RSA key pairs with a 2048-bit modulus in accordance with FIPS PUB 186-4.

The TOE supports IPsec AH and ESP using AES (CBC) with 128, 192 or 256 bit keys and HMAC-SHA-1-96.

The TOE supports RSA encryption, which is used to verify certificates that identify itself and peers in IPsec and SSH negotiations. The TOE does not generate certificates.

Additionally, the TOE is designed to zeroize the cryptographic keys of all types when they are no longer required by the TOE, in a manner designed to conform to FIPS 140-2.

The Cryptographic Support function satisfies the following security functional requirements:

- FCS_CKM.1—the TOE generates RSA key pairs with a 2048-bit modulus.
- FCS_CKM.4—the TOE zeroizes cryptographic keys when they are no longer needed.
- FCS_COP.1(1)—the TOE implements AES using CBC mode to support its secure IPsec and SSHv2 protocols.
- FCS_COP.1(2)—the TOE provides digital signature generation and verification services using RSA with 2048-bit modulus.
- FCS_COP.1(3)—the TOE implements SHA-1, SHA-256 and SHA-512 cryptographic hash algorithms to support SSHv2 and IPsec.
- FCS_COP.1(4)—the TOE implements HMAC-SHA-1 and HMAC-SHA-1-96 for use with SSHv2 and IPsec.
- FCS_COP.1(5)—the TOE (depending on the device model) implements an ANSI X9.31 random number generator (HSR6600/HSR6800 Series) or a CTR_DRBG(AES) random bit generator (MSR1000 Series) to support generation of RSA key pairs and AES keys.

6.3 User Data Protection

The TOE provides firewall capabilities that allow for the definition of firewall rules, collectively known as access control lists (ACLs), which are applied to applicable network traffic as it is received and which would pass through the TOE between connected networks. The ACLs can be basic, with matching criteria based only on source IP address, or advanced, with matching criteria based on source and destination addresses, transport layer protocol, and service. ACLs can also be defined independently for both IPv4 and IPv6 network traffic and can be assigned to specific TOE interfaces.

Basic ACLs define matching criteria in terms of source IPv4 or IPv6 addresses and allowable times and support permit and deny operations.

Advanced ACLs define matching criteria in terms of IPv4 and IPv6 packet header attributes: source and destination addresses; source and destination ports; transport layer protocol; TCP header flags (ACK, FIN, PSH, RST, SYN, URG), and ICMP type. The ACLs also support permit and deny operations.

In each case, ACL ordering can be selected by a user in the network-admin role to be either as configured (i.e., rules are processed in the order they are defined by the network-admin) or automatic, in which case the rules are automatically sorted in a depth-first order so that the most specific matching criteria is applied first with some tie-breaking heuristics to resolve equal specificity.

Once ACLs are defined, the TOE will process all network traffic against the configured ACLs. The rules in the applicable ACLs are processed in the specified order until a match is encountered and the operation associated with that matching rule (permit or deny) will be enforced. If there is no match, the traffic by default will be permitted. This can be changed to default deny by a CLI command (**packet-filter default deny**).

The User Data Protection function satisfies the following security functional requirements:

- FDP_IFC.1—the TOE implements an unauthenticated information flow security functional policy (i.e., firewall policy) that applies to all network traffic that would flow through the TOE between connected networks.
- FDP_IFF.1—the TOE provides a flexible set of firewall rules that can be employed to permit or deny network traffic that would flow through the TOE based on source and destination addresses, source and destination ports, transport layer protocol, TOE interface (where networks are defined), ICMP type and other header information.

6.4 Identification and Authentication

The TOE requires authorized users to be identified and authenticated before they can access any of the TOE functions. Note that the normal routing of network traffic is not considered accessing TOE functions in this regard.

In the evaluated configuration, users can connect to the TOE CLI via a local console or remotely using SSHv2. In both cases, the user is required to log in prior to successfully establishing a session through which TOE functions can be exercised.

In order to log in at the console or via SSH, the user must provide an identity and also authentication data that matches the provided identity (e.g., password or password with RSA credentials used in conjunction with an SSH session). Users can be defined locally within the TOE with a user identity, password, and role(s). Once a locally defined user logs in, they can optionally provide RSA credentials (i.e., their public key) that the TOE will store for use with subsequent SSH credential based authentication. When a user public-key is configured, the TOE requires both the RSA credentials and the user's password for authentication. Use of the SSHv2 protocol is required in order for authentication to use both a password and RSA credential for login. Earlier versions of SSH do not support authentication using both mechanisms.[2]

Alternately, users can be defined within an external RADIUS or TACACS+ server configured to be used by the TOE, each of which also defines the user's role in the TOE. Locally defined users are authenticated directly by the TOE, while remotely defined users are authenticated by the external server and the result is enforced by the TOE. In either case, any resulting session is dependent upon successful authentication and established sessions are associated with the privilege level/role (see Section 6.5) assigned to the user.

By default, only local authentication will be used, but a user in the network-admin role can specifically identify the authentication mechanisms (local, RADIUS, and/or TACACS+) to be used, as well as the order in which they will be checked. If a configured authentication service is not available (e.g., RADIUS server cannot be reached), the TOE will use the next configured authentication mechanism.

In any case, the user is authenticated either by the local[3], RADIUS or TACACS+ mechanism. Every session is dependent upon successful authentication. Established sessions are associated with the role(s) assigned to the authenticated user.

The TOE requires that passwords used for authentication must be at least 15 characters in length (up to 63 characters are supported) and must include at least one each of: lower case alphabetic characters, upper case alphabetic characters, numbers, and special characters.

Note also that should a console user have their session locked (e.g., due to inactivity), they are required to successfully re-authenticate, by re-entering their identity and authentication data, in order to regain access to their locked session.

If a user fails to log in a network-admin configured number of times in a row, the user (unless the user identity is not defined) is added to a blacklist. The TOE can be configured to operate in one of the following ways:

- The TOE can be configured to prohibit the user from logging in until the user is manually removed from the blacklist.
- The TOE can be configured to prohibit the user from logging in for a configurable period of time, allowing the user to log in again after that time has lapsed or the user has been manually removed from the black list (i.e., by a network-admin).
- The TOE can be configured to allow the user to continue trying to log in until the user successfully authenticates. Note that this setting effectively disables the blacklist feature.

User accounts for users in the security-audit role are not locked as a result of failed logins. Such users are not under the locking control because they are responsible for monitoring activity within the TOE.

[2] When the TOE is configured in FIPS mode, SSHv2 authentication using only RSA credentials is not allowed. The TOE must be operating with FIPS mode disabled in order to support public key only authentication over SSHv2.
[3] Local authentication for SSH can be password-based, certificate-based or both.

When logging in, the TOE will not echo passwords so that passwords are not inadvertently displayed to the user and any other users that might be able to view the login display.

The Identification and Authentication function satisfies the following security functional requirements:

- FIA_AFL.1—a user in the network-admin role can configure a non-zero threshold for authentication failures that can occur before the TOE takes action to prevent subsequent authentication attempts. The TOE can be configured to disable the user until a user in the network-admin role takes an explicit action to change that. However, the TOE offers other options (summarized above) for operational environments where that may not be necessary.
- FIA_ATD.1—locally defined users are assigned identities, passwords, and role(s).
- FIA_SOS.1—the TOE requires passwords to be at least 15 characters long and to have a variety of characters as indicated above.
- FIA_UAU.2—the TOE does not provide any services or access to its functions until after the user is successfully authenticated.
- FIA_UAU.5—the TOE supports the use of TACACS and RADIUS in addition to passwords or passwords with certificates to be used for user authentication as described above.
- FIA_UAU.7—the TOE provides only obscured feedback during user authentication.
- FIA_UID.2—the TOE does not offer any services or access to its functions until after the user is successfully identified.

6.5 Security Management

The TOE implements a role mechanism that is used to specify the role(s) and corresponding permissions which authenticated users possess. Table 6 identifies and describes the predefined roles that are implemented by the TOE and their corresponding permissions.

Users with the network-admin or level-15 role correspond to and can perform all of the operations of the Network Administrator role from FMT_SMR.1. Users with the network-operator or level-9 role can perform only some of the management functions assigned to the Network Administrator role (e.g., the network-operator role can perform display operations). Users with level-2 through level-8 and level-10 through level-14 have no default permissions.

User Role	Permissions
network-admin	Accesses all features and resources in the system, except for the **display security-logfile summary**, **info-center security-logfile directory**, and **security-logfile save** commands (equivalent to level-15)
security-audit	Has the following access to security log file (`seclog.log`): • Access to the commands for displaying and maintaining the `seclog.log` file (for example, the **dir**, **display security-logfile summary**, and **more** commands). • Access to the commands for managing the `seclog.log` file and the `seclog.log` file system (for example, the **info-center security-logfile directory**, **mkdir**, and **security-logfile save** commands). Only the security-audit role has access to the `seclog.log` file.
network-operator	Accesses the **display** commands for all features and resources in the system, except for commands such as **display history-command all** and **display security-logfile summary**. Enables local authentication login users to change their own password. (equivalent to level-1)

User Role	Permissions
level-n (n = 0 to 15)	level-0—has access to diagnostic commands, including **ping**, **tracert**, **ssh2**, **telnet**, and **super**. Level-0 access rights are configurable. level-1—has access to the display commands of all features and resources in the system except **display history-command all**. The level-1 user role also has all access rights of the user role level-0. Level-1 access rights are configurable. level-2 to level-8, and level-10 to level-14—have no access rights by default. Access rights are configurable. level-9—has access to all features and resources except those in the following list: o RBAC non-debugging commands o Local users o File management o Device management o The **display history-command all** command. A local user account that has a level-9 user role can change the password in the local user account. Level-9 access rights are configurable. level-15—Has the same rights as network-admin.

Table 6: Security Management Role Definitions

The level-0 through level-14 and network-operator roles are not needed in order to properly administer the TOE. These roles possess a subset of the permissions of the network-admin role and thus are capable of only some of the management functions available to the network-admin role. These additional user roles (e.g., level-9, network-operator) can be combined to grant the user all permissions provided by the combined set of roles.

The CLI provides access to the TOE's security management functions. The following functions are limited to the network-admin role:

- Manage the firewall rules—create, modify, and delete information flow security policy rules (ACLs) that permit or deny information flows
- Manage user account definitions—create, modify, and delete user attributes that identify authorized users and their associated role(s), and restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures
- Manage password controls—enable and modify rules for password composition (length, required characters) and the threshold for the number of permitted authentication attempt failures
- Manage the internal clock—modify and set the time and date
- Manage remote authentication capabilities—enable, disable, and configure external RADIUS and TACACS+ services.

The Security Management function satisfies the following security functional requirements:

- FMT_MOF.1—the TOE restricts the ability to manage remote authentication capabilities to users in the network-admin role.
- FMT_MSA.1—the TOE restricts the ability to modify the information flow rules to a user in the network-admin role.
- FMT_MSA.3—the TOE implements a permissive default firewall policy by permitting network traffic when there are no matching rules. Only a network-admin can change that default, either by defining rules that are capable of matching and taking specifically configured actions for all network traffic the TOE might receive, or by changing to default deny using the **packet-filter default deny** CLI command.
- FMT_MTD.1(1)—the TOE restricts the ability to clear and archive the audit trail to users in the network-admin role.

- FMT_MTD.1(2), FMT_MTD.1(3)—the TOE restricts the ability to manage user accounts, password controls, and the system clock to users in the network-admin role.
- FMT_SMF.1—the TOE provides the capabilities necessary to manage the security of the TOE.
- FMT_SMR.1—"Network Administrator" corresponds to users in the TOE predefined role of network-admin or level-15. A "Network Operator" corresponds to users in the TOE predefined role of network-operator.

6.6 Protection of the TSF

The HSR6600 and HSR6800 Series devices include a hardware-based real-time clock (RTC). The RTC is a battery-powered clock that is included in a microchip in a computer motherboard. When a device starts up, the device gets the time from the RTC and synchronizes it to the CPU. When the device is powered off, the RTC still keeps track of the current time.

The MSR1000 Series devices do not have an RTC. Instead, these devices maintain time by adding CPU ticks to the default time of the system.

The TOE's embedded OS manages the system clock (whether based on RTC or CPU ticks) and exposes administrator clock-related functions. The clock is used for audit record time stamps, measuring session inactivity for termination, and for cryptographic operations based on time/date. The TOE can also be configured to use the Network Time Protocol to keep the system clock synchronized with other network devices.

The TOE includes a number of built in diagnostic tests that are run during start-up to determine whether the TOE is operating properly. An administrator can configure the TOE to reboot or to stop, with errors displayed, when an error is encountered. The built-in self-tests include basic read-write memory (that is, each memory location is written with a non-zero value and read to ensure it is stored as expected), flash read, software checksum tests, and device detection tests. When operating in CC/FIPS mode, the power-on self-tests comply with the FIPS 140-2 requirements for self-testing.

The Protection of the TSF function satisfies the following security functional requirements:

- FPT_STM.1—the TOE manages a system clock that can be set locally by a network-admin or synchronized with other devices using NTP.
- FPT_TST.1—the TOE includes a number of power-on diagnostics that will serve to ensure the TOE is functioning properly. The tests include ensure memory and flash can be accessed as expected, to ensure that software checksums are correct, and also to test the presence and function of plugged devices.

6.7 TOE Access

The TOE can be configured by a user in the network-admin role to set an interactive session timeout value (any integer value in minutes and also optionally in seconds, with 0 disabling the timeout) – the default timeout is 10 minutes. A remote session that is inactive (that is, no commands issuing from the remote client) for the defined timeout value will be terminated. A local session that is similarly inactive for the defined timeout period will be terminated. The user will be required to enter their user id and their password so they can establish a new session once a session is terminated. If the user id and password match those of the user that was locked, the session is reconnected with the console and normal input/output can again occur for that user.

The TOE Access function satisfies the following security functional requirements:

- FTA_SSL.3—the TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- FTA_SSL.4—the TOE provides the function to logout (or terminate) both local and remote user sessions as directed by the user.

6.8 Trusted Path/Channels

The TOE supports communications via trusted channels with other trusted IT products for the following functions:

- Export of generated audit records to an external syslog server
- Authentication of users defined in an external RADIUS or TACACS server.

The trusted channel to both a syslog server and an authentication server is established using IPsec. The TOE implements IKEv1 for key establishment and Encapsulating Security Payload (ESP) to provide confidentiality, data origin authentication, and integrity between itself and the external server.

The TOE provides a trusted path for administrators of the TOE to communicate with the TOE. The trusted path is implemented using SSHv2 to access the CLI. Administrators initiate the trusted path by establishing an SSH session using an SSH client. The TOE implements SSHv2 using 2048-bit RSA keys for digital signature generation and verification, 128 or 256-bit AES keys for session data encryption and decryption, and HMAC-SHA-1 or HMAC-SHA-1-96 for data authentication.

The trusted path is used for initial authentication and all subsequent administrative actions. The use of SSHv2 ensures all communication over the trusted path is protected from disclosure and undetected modification.

The Trusted Path/Channels function satisfies the following security functional requirements:

- FTP_ITC.1—the TOE can be configured to ensure that any authentication operations and exported audit records are sent only to the configured servers via IPsec communications channels so they are not subject to inappropriate disclosure or modification.
- FTP_TRP.1—the TOE provides a trusted path for administrators to communicate with the TOE, using SSHv2 to access the CLI.

7. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Requirement Dependencies
- TOE Summary Specification.

7.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives for the TOE or operational environment. In addition, each objective counters or addresses at least one assumption or threat.

	T.BRUTE_FORCE	T.MEDIATE	T.NETWORK_COMPROMISE	T.NO_ACCOUNTABILITY	T.UNATTENDED_SESSION	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_ACTIVITY	A.PROTECT	A.MANAGE	A.NOEVIL
O.AUDIT				X						
O.AUDIT_REVIEW				X						
O.AUDIT_STORAGE				X						
O.CRYPTOGRAPHY			X							
O.I_&_A						X				
O.MEDIATE		X								
O.PASSWORD_CONTROLS	X									
O.PROTECTED_COMMS			X							
O.SECURITY_MANAGEMENT							X			
O.SESSION_TERMINATION					X					
O.THROTTLE	X									
OE.PHYSICAL								X		
OE.PERSONNEL									X	X

Table 7: Security Problem Definition to Security Objective Correspondence

7.1.1.1 T.BRUTE_FORCE

An unauthorized user may gain access to the TOE through repeated password-guessing attempts.

This threat is countered by the following security objectives:

- O.PASSWORD_CONTROLS—addresses this threat by providing a mechanism, configurable by an administrator, which encourages users to choose difficult-to-guess passwords.

- O.THROTTLE—addresses this threat by limiting the number of passwords that can be guessed for a single account to a rate of six per minute.

7.1.1.2 T.MEDIATE

An unauthorized IT entity may send information through the TOE to compromise IT entities on an internal (protected) network.

This threat is countered by the following security objective:

- O.MEDIATE—addresses this threat by ensuring the TOE mediates the flow of information from IT entities on one connected network to IT entities on another connected network.

7.1.1.3 T.NETWORK_COMPROMISE

TSF data communicated between the TOE and external entities is disclosed or undetectably modified.

This threat is countered by the following security objectives:

- O.PROTECTED_COMMS—addresses this threat by ensuring all communications between the TOE and external entities are protected using cryptographic protocols, such as SSH and IPsec.
- O.CRYPTOGRAPHY—supports O.PROTECTED_COMMS by ensuring the TOE implements the cryptographic algorithms necessary to support the cryptographic protocols that satisfy O.PROTECTED_COMMS.

7.1.1.4 T.NO_ACCOUNTABILITY

Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.

This threat is countered by the following security objectives:

- O.AUDIT—addresses this threat by ensuring the TOE is able to generate audit records of security relevant events.
- O.AUDIT_REVIEW—supports O.AUDIT in addressing the threat by ensuring the TOE provides capabilities for effective review of stored audit records.
- O.AUDIT_STORAGE—supports O.AUDIT in addressing the threat by ensuring the TOE protects stored audit records from unauthorized modification and deletion.

7.1.1.5 T.UNATTENDED_SESSION

An unauthorized user gains access to the TOE via an unattended authorized user session.

This threat is countered by the following security objective:

- O.SESSION_TERMINATION—addresses this threat by providing users with a mechanism to terminate their interactive sessions with the TOE, and by ensuring sessions that have been inactive for a configurable period of time will be terminated by the TOE.

7.1.1.6 T.UNAUTHORIZED_ACCESS

Unauthorized users gain access to the TOE and its services.

This threat is countered by the following security objective:

- O.I_AND_A—addresses this threat by ensuring all users of the TOE are identified and authenticated prior to gaining further access to the TOE and its services.

7.1.1.7 T.UNAUTHORIZED_ACTIVITY

Authorized users perform unauthorized actions on the TOE.

This threat is countered by the following security objective:

- O.SECURITY_MANAGEMENT—addresses this threat by providing a mechanism that requires authorized users to have appropriate privileges in order to perform actions on the TOE.

7.1.1.8 A.PROTECT

The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

This assumption is satisfied by the following security objective:

- OE.PHYSICAL—this objective satisfies the assumption by ensuring the TOE is protected from physical attack.

7.1.1.9 A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This assumption is satisfied by the following security objective:

- OE.PERSONNEL—this objective satisfies the assumption by ensuring those assigned as authorized administrators are properly trained in operating the TOE.

7.1.1.10 A.NOEVIL

The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

This assumption is satisfied by the following security objective:

- OE.PERSONNEL—this objective satisfies the assumption by ensuring those assigned as authorized administrators are carefully selected for the job and are properly trained in operating the TOE.

7.2 Security Functional Requirements Rationale

All security functional requirements identified in this Security Target are fully addressed in this section and each is mapped to the objective it is intended to satisfy. Table 8 summarizes the correspondence of functional requirements to TOE security objectives.

	O.AUDIT	O.AUDIT_REVIEW	O.AUDIT_STORAGE	O.CRYPTOGRAPHY	O.MEDIATE	O.I_AND_A	O.PASSWORD_CONTROLS	O.PROTECTED_COMMS	O.SECURITY_MANAGEMENT	O.SESSION_TERMINATION	O.THROTTLE
FAU_GEN.1	X										
FAU_GEN.2	X										
FAU_SAR.1		X									
FAU_SAR.3		X									
FAU_STG.1			X								
FAU_STG.4			X								
FCS_CKM.1				X							

	O.AUDIT	O.AUDIT_REVIEW	O.AUDIT_STORAGE	O.CRYPTOGRAPHY	O.MEDIATE	O.I_AND_A	O.PASSWORD_CONTROLS	O.PROTECTED_COMMS	O.SECURITY_MANAGEMENT	O.SESSION_TERMINATION	O.THROTTLE
FCS_CKM.4				X							
FCS_COP.1(*)				X							
FDP_IFC.1					X						
FDP_IFF.1					X						
FIA_AFL.1											X
FIA_ATD.1						X					
FIA_SOS.1							X				
FIA_UAU.2						X					
FIA_UAU.5						X					
FIA_UAU.7						X					
FIA_UID.2						X					
FMT_MOF.1(*)									X		
FMT_MSA.1					X						
FMT_MSA.3					X						
FMT_MTD.1(*)									X		
FMT_SMF.1									X		
FMT_SMR.1									X		
FPT_STM.1	X										
FPT_TST.1				X							
FTA_SSL.3										X	
FTA_SSL.4										X	
FTP_ITC.1								X			
FTP_TRP.1								X			

Table 8: Objectives to Requirement Correspondence

7.2.1.1 O.AUDIT

The TOE shall be able to generate audit records of security-relevant events, identifying users causing the events as applicable.

The following security functional requirements contribute to satisfying this security objective:

- FAU_GEN.1—the ST includes FAU_GEN.1 to specify the capability to generate audit records of security-relevant events, and to specify the specific events to be audited and the content of generated audit records of those events.
- FAU_GEN.2—the ST supports FAU_GEN.1 by including FAU_GEN.2 to specify the capability to include, when applicable, the identity of the user associated with the auditable event.
- FPT_STM.1—the ST supports FAU_GEN.1 by including FPT_STM.1 to specify the capability for the TOE to provide reliable time stamps, which are used by the TOE when generating audit records

7.2.1.2 O.AUDIT_REVIEW

The TOE shall provide a means for authorized users to review the audit records generated by the TOE.

The following security functional requirement contributes to satisfying this security objective:

- FAU_SAR.1—the ST includes FAU_SAR.1 to specify which roles are to be able to read data from stored audit records.
- FAU_SAR.3—the ST supports FAU_SAR.1 by including FAU_SAR.3 to specify capabilities for searching stored audit records and the criteria by which searches can be performed.

7.2.1.3 O.AUDIT_STORAGE

The TOE shall protect stored audit records from unauthorized modification and deletion and shall provide a means to prevent the loss of audit records in the event the space available for storing them is exhausted.

The following security functional requirement contributes to satisfying this security objective:

- FAU_STG.1—the ST includes FAU_STG.1 to specify that stored audit records are to be protected from unauthorized modification or deletion.
- FAU_STG.4—the ST includes FAU_STG.4 to specify capabilities to prevent the loss of generated audit records if the audit trail is full.

7.2.1.4 O.CRYPTOGRAPHY

The TOE shall perform cryptographic operations to support protocols used to protect data in transit.

The following security functional requirements contribute to satisfying this security objective:

- FCS_COP.1(*)—the ST includes iterations of FCS_COP.1 to specify the cryptographic algorithms implemented by the TOE to support cryptographic protocols.
- FCS_CKM.1—the ST supports FCS_COP.1(2) by including FCS_CKM.1 to specify the capability to generate RSA key pairs of appropriate size.
- FCS_CKM.4—the ST supports FCS_COP.1(*) by including FCS_CKM.4 to specify the capability to destroy cryptographic keys when they are no longer required.

7.2.1.5 O.I_AND_A

The TOE shall require all users of the TOE to be identified and authenticated before gaining access to TOE services.

The following security functional requirements contribute to satisfying this security objective:

- FIA_UID.2, FIA_UAU.2—the ST includes FIA_UID.2 and FIA_UAU.2 to specify that users must be successfully identified and authenticated by the TOE before being able to perform any other TSF-mediated actions.
- FIA_ATD.1—the ST supports FIA_UID.2 and FIA_UAU.2 by including FIA_ATD.1 to ensure user identity and authentication data security attributes are associated with individual users.
- FIA_UAU.5—the ST supports FIA_UAU.2 by including FIA_UAU.5 to specify multiple authentication mechanisms that are supported by the TOE.
- FIA_UAU.7—the ST supports FIA_UAU.2 by including FIA_UAU.7 to specify that only obscured feedback is provided during the authentication process, reducing the likelihood of a user's password being exposed to unauthorized users.

7.2.1.6 O.MEDIATE

The TOE shall mediate the flow of information from IT entities on one connected network to IT entities on another connected network.

The following security functional requirements contribute to satisfying this security objective:

- FDP_IFC.1, FDP_IFF.1—the ST includes FDP_IFC.1 and FDP_IFF.1 to specify the information flow control policy enforced by the TOE to mediate the flow of information between IT entities on external and internal networks.
- FMT_MSA.1, FMT_MSA.3—the ST includes FMT_MSA.1 and FMT_MSA.3 to specify restrictions on the management of security attributes used to mediate the flow of information between IT entities on external and internal networks.

7.2.1.7 O.PASSWORD_CONTROLS

The TOE shall provide a mechanism to reduce the likelihood that users choose weak passwords.

The following security functional requirements contribute to satisfying this security objective:

- FIA_SOS.1—the ST includes FIA_SOS.1 to specify that passwords must meet minimum construction requirements, in terms of length and character set.

7.2.1.8 O.PROTECTED_COMMS

The TOE shall protect communications between the TOE and external entities from disclosure and undetected modification.

The following security functional requirements contribute to satisfying this security objective:

- FTP_ITC.1, FTP_TRP.1—the ST includes FTP_ITC.1 and FTP_TRP.1 to specify that communications between the TOE and external entities will be protected from disclosure and undetected modification.

7.2.1.9 O.SECURITY_MANAGEMENT

The TOE shall restrict the ability to perform security management functions on the TOE to authorized administrators having appropriate privileges.

The following security functional requirements contribute to satisfying this security objective:

- FMT_SMF.1, FMT_SMR.1, FMT_MOF.1(*), FMT_MTD.1(*)—the ST includes these requirements to specify the security management functions to be provided by the TOE (FMT_SMF.1), to specify security management roles and privileges (FMT_SMR.1), and to specify the restrictions on management of security function behavior and TSF data (FMT_MOF.1(*), FMT_MTD.1(*)).

7.2.1.10 O.SESSION_TERMINATION

The TOE shall provide mechanisms to terminate a user session after a period of inactivity or at the request of the user.

The following security functional requirements contribute to satisfying this security objective:

- FTA_SSL.3—the ST includes FTA_SSL.3 to specify the capability for the TSF to terminate an interactive user session after a period of inactivity.
- FTA_SSL.4—the ST includes FTA_SSL.4 to specify the capability for users to terminate their own interactive sessions.

7.2.1.11 O.THROTTLE

The TOE shall limit the rate at which consecutive unsuccessful authentication attempts can be performed.

The following security functional requirement contributes to satisfying this security objective:

- FIA_AFL.1—the ST includes FIA_AFL.1 to specify the capability to limit the rate at which consecutive failed authentication attempts (which may indicate a password-guessing attack) can be made.

7.3 Security Assurance Requirements Rationale

EAL3 was selected as the assurance level because the TOE is a commercial product whose users require a moderate level of independently assured security. The TOE is targeted at an environment with good physical access security where it is assumed that attackers will have Basic attack potential. Augmentation was chosen to provide the added assurance that is gained by defining flaw remediation and flaw reporting procedures. Therefore, the target assurance level of EAL3 augmented with ALC_FLR.2 is appropriate for such an environment.

7.4 Requirement Dependency Rationale

The following table identifies the SFRs claimed in the ST, their dependencies as defined in CC Part 2, and how the dependency is satisfied in the ST. It can be seen that all dependencies have been satisfied by inclusion in the ST of the appropriate dependent SFRs.

Requirement	Dependencies	How Satisfied
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1,
	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1)
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1(*)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1	FDP_IFC.1
	FMT_MSA.3	FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 (hierarchical to FIA_UAU.1)
FIA_ATD.1	None	n/a
FIA_SOS.1	None	n/a
FIA_UAU.2	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1)
FIA_UAU.5	None	n/a
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2 (hierarchical to FIA_UAU.1)
FIA_UID.2	None	n/a
FMT_MOF.1(*)	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1
	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	FMT_SMR.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1(*)	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	None	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1)
FPT_STM.1	None	n/a
FPT_TST.1	None	n/a
FTA_SSL.3	None	n/a

Requirement	Dependencies	How Satisfied
FTA_SSL.4	None	n/a
FTP_ITC.1	None	n/a
FTP_TRP.1	None	n/a

Table 9: Requirement Dependencies

7.5 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functional requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

The following table provides a mapping of the SFRs to the security function descriptions to support the TOE Summary Specification.

	Security Audit	Cryptographic Support	User Data Protection	Identification and Authentication	Security Management	Protection of the TSF	TOE Access	Trusted Path/Channels
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_SAR.1	X							
FAU_SAR.3	X							
FAU_STG.1	X							
FAU_STG.4	X							
FCS_CKM.1		X						
FCS_CKM.4		X						
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						
FCS_COP.1(3)		X						
FCS_COP.1(4)		X						
FCS_COP.1(5)		X						
FDP_IFC.1			X					
FDP_IFF.1			X					
FIA_AFL.1				X				
FIA_ATD.1				X				
FIA_UAU.2				X				
FIA_UAU.5				X				
FIA_UAU.7				X				
FIA_UID.2				X				
FMT_MOF.1					X			
FMT_MSA.1					X			
FMT_MSA.3					X			
FMT_MTD.1					X			
FMT_SMF.1					X			
FMT_SMR.1					X			
FPT_STM.1						X		
FPT_TST.1						X		
FTA_SSL.3							X	
FTA_SSL.4							X	
FTP_ITC.1								X
FTP_TRP.1								X

Table 10: Security Functions vs. Requirements Mapping

Appendix A: Documentation for Hewlett Packard Enterprise HSR6600, HSR6800, and MSR1000 Series Routers

This Appendix provides a list of the product documentation used during the evaluation of each Hewlett Packard Enterprise HSR6600, HSR6800, and MSR1000 Series router product family.

A.1 HSR6600 Router Series

The following documents for the HSR6600 Router Series can be found under the *General reference* and *Setup and install- general* sections of the HSR6600 Router Series documentation page on the Hewlett Packard Enterprise Web site, at this URL:

http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=5354492&ac.admitted=1455807485582.125225703.1938120508#manuals

- HPE FlexNetwork 6600/HSR6600 Routers Security Configuration Guide
- HPE FlexNetwork 6600/HSR6600 Routers Security Command Reference
- HPE FlexNetwork 6600/HSR6600 Routers Fundamentals Configuration Guide
- HPE FlexNetwork 6600/HSR6600 Routers Fundamentals Command Reference
- HPE FlexNetwork 6600/HSR6600 Routers Network Management and Monitoring Configuration Guide
- HPE FlexNetwork 6600/HSR6600 Routers Network Management and Monitoring Command Reference
- HPE FlexNetwork 6600/HSR6600 Routers ACL and QoS Configuration Guide
- HPE FlexNetwork 6600/HSR6600 Routers ACL and QoS Command Reference
- HPE FlexNetwork 6600/HSR6600 Routers Layer 3—IP Services Configuration Guide
- HPE FlexNetwork 6600/HSR6600 Routers Layer 3—IP Services Command Reference
- HP HSR6600 Routers Installation Guide

A.2 HSR6800

The following documents for the HSR6800 Router Series can be found under the *General reference* and *Setup and install- general* sections of the HSR6800 Router Series documentation page on the Hewlett Packard Enterprise Web site, at this URL:

http://h20565.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=5365643&ac.admitted=1455810410725.125225703.1851288163#manuals

- HPE FlexNetwork HSR6800 Routers Security Configuration Guide
- HPE FlexNetwork HSR6800 Routers Security Command Reference
- HPE FlexNetwork HSR6800 Routers Fundamentals Configuration Guide
- HPE FlexNetwork HSR6800 Routers Fundamentals Command Reference
- HPE FlexNetwork HSR6800 Routers Network Management and Monitoring Configuration Guide
- HPE FlexNetwork HSR6800 Routers Network Management and Monitoring Command Reference
- HPE FlexNetwork HSR6800 Routers ACL and QoS Configuration Guide
- HPE FlexNetwork HSR6800 Routers ACL and QoS Command Reference
- HPE FlexNetwork HSR6800 Routers Layer 3—IP Services Configuration Guide
- HPE FlexNetwork HSR6800 Routers Layer 3—IP Services Command Reference
- HP HSR6800 Routers Installation Guide

A.3 MSR1000

The following documents for the MSR1000 Router Series can be found under the *General reference* and *Setup and install- general* sections of the MSR1000 Router Series documentation page on the Hewlett Packard Enterprise Web site, at this URL:

http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=6796027&ac.admitted=1451955288924.125225703.1938120508#manuals

- HP MSR Router Series Security Configuration Guide(V7)
- HP MSR Router Series Security Command Reference(V7)
- HP MSR Router Series Fundamentals Configuration Guide(V7)
- HP MSR Router Series Fundamentals Command Reference(V7)
- HP MSR Router Series Network Management and Monitoring Configuration Guide(V7)
- HP MSR Router Series Network Management and Monitoring Command Reference(V7)
- HP MSR Router Series ACL and QoS Configuration Guide(V7)
- HP MSR Router Series ACL and QoS Command Reference(V7)
- HP MSR Router Series Layer 3—IP Services Configuration Guide(V7)
- HP MSR Router Series Layer 3—IP Services Command Reference(V7)
- HP MSR1000 Routers Installation Guide