HP Routers EAL2 Security Target

Version: 1.07

Aug. 20, 2010

Prepared by: Hewlett-Packard Development Company, L.P.

Revision History:

Version	Date of Release	Reasons for change	Author
V1.0	2009-05-27	Initial	HP
V1.01	2009-06-30	The document was revised according to the review comments on ASE_ST_3Com_150609.doc.	HP
V1.02	2009-08-05	The document was revised according to the review comments on OR_ASE_R_29072009.doc.	HP
V1.03	2009-09-08	1) The document was revised according to the observation report *OR_ASE_20082009.doc*. 2) The TOE security function was changed to provide the log server function, and logs are saved on the log server. Because the log server is not in the TOE boundary, components FAU_SAR.1 and FAU_STG.1 were deleted. Additionally, the description of OE.INTEROPERABILITY was modified. Section 7 TOE Summary Specification and section 8 Rationales were modified accordingly.	HP
V1.04	2009-11-29	FAU_SAR.1 and FAU_STG.1 were added.	HP

V1.05	2010-03-11	The document was revised according to the review comments on OR_ASE_0522010.doc.	HP
V1.06	2010-04-19	Del ALC_LCD,ALC_DVS, ALC_FLR	HP
V1.07	2010-08-20	The document was revised according to the review comments from STQC.	HP

Table of Contents

Figure List

Table List

List of abbreviations:

Abbreviations	Full spelling
BGP	Border Gateway Protocol
RIP	Routing Information Protocol
OSPF	Open Shortest Path Protocol
AAA	Authentication, Authorization, Accounting
RADIUS	Remote Authentication Dial In User Service
CLI	Command Line Interface
iMC	Intelligent Management Center
TOE	Target of Evaluation
SFP	Security Functions Policy
SFR	Security Functions Requirements

1 ST Introduction

This section identifies the ST, TOE, conformance claims, and document conventions.

1.1 ST Reference Identification

ST identification: HP Routers EAL2 Security Target

- Version: 1.07
- Prepared on: August 20, 2010
- Prepared by: Hewlett-Packard Development Company, L.P.

1.2 TOE Reference Identification

TOE identification: The TOE is the network Operating System software (NOS), Comware V5.2 release no. 1002(CC) running on MSR 20, MSR 30, MSR 50 , SR 66 and SR 88 series routers. The router hardware act as environment to the TOE.

Table 1-1 TOE running on following Routers(IT environment)

Series	Products
MSR 20 Series	MSR 20-10, MSR 20-11, MSR 20-12, MSR 20-13, MSR 20-15, MSR 20-20, MSR 20-21, MSR 20-40
MSR 30 Series	MSR 30-10, MSR 30-11, MSR 30-11E, MSR 30-11F, MSR 30-16, MSR 30-20, MSR 30-40, MSR 30-60
MSR 50 Series	MSR 50-40, MSR 50-60, MSR 50-40 MPU-G2, MSR 50-60 MPU-G2
SR 66 Series	SR6602, SR6604, SR6608, SR6616
SR 88 Series	SR8802, SR8805, SR8808, SR8812

TOE developers: Chen Guanghui, Chen Weifeng, Sun Ludong, Chang Huifeng, Hu Xiaolong, Li Yongbo, Chen Guohua

1.3 TOE Overview

1.3.1 Usage and major security features of the TOE

The TOE is the network Operating System software (NOS), Comware V5.2 release no. 1002(CC) running on MSR 20, MSR 30, MSR 50 , SR 66 and SR 88 series routers. The router hardware act as environment to the TOE.The TOE is exclusively developed by HP, and it boasts high reliability, good configurability, and rich network features.

Routers are hardware devices that can be used to connect different types of networks or network segments, and are mainly used to forward packets between networks or network segments.

The major TOE security functions are described in 1.4.2.

1.3.2 TOE Type

The TOE is the network Operating System software (NOS), Comware V5.2 release no. 1002(CC) running on MSR 20, MSR 30, MSR 50 , SR 66 and SR 88 series routers. The TOE provides a wide variety of services. Users of the TOE fall into two types: the first type is users using the data communication services of the TOE, referred to as network users; the second type is users performing system configuration management for the TOE, referred to as device administrators or system administrators. The network users cannot manage the TOE. They can only use the data communication services provided by the TOE in the security environments defined by the system administrator. Therefore, only the behaviors of the system administrators can affect the usage of TSF. A system administrator can log in locally through the local management interface (Console port or AUX port) of the router or remotely through SSH, and then use the CLI to configure security functions.

1.3.3 Required non-TOE hardware/software/firmware

The TOE must be configured in the network environment described in 1.4.1 and the soft/hard devices forming the network environment.

The following hardware/software/firmware of non-TOE should be acquired additionally:

- HP iMC software
- Windows 2000 server or Linux server, where HP iMC can run
- NTP server, which may be required when a router has no hardware clock
- A log server as needed
- SSH client software

1.4 TOE Description

The TOE is the network Operating System software (NOS), Comware V5.2 release no. 1002(CC) running on MSR 20, MSR 30, MSR 50 , SR 66 and SR 88 series routers. The router hardware act as

environment to the TOE. The routing, forwarding, and control functions on all these routers are separated to achieve network management flexibility and security control while high-performance data communication services are guaranteed.

MSR series routers: the MSR series routers include the MSR 20 series, 30 series, and 50 series, with their target markets ascending from low end to high end. The MSR 20 and MSR 30 series routers can operate as the edge access routers in large-sized networks or service provider networks, or operate as core routers in networks of branches or small-sized enterprises; the MSR 50 series routers can operate as core routers in large-/medium-sized enterprise networks, or operate as edge, distribution, or access devices in large-sized networks or service provider networks.

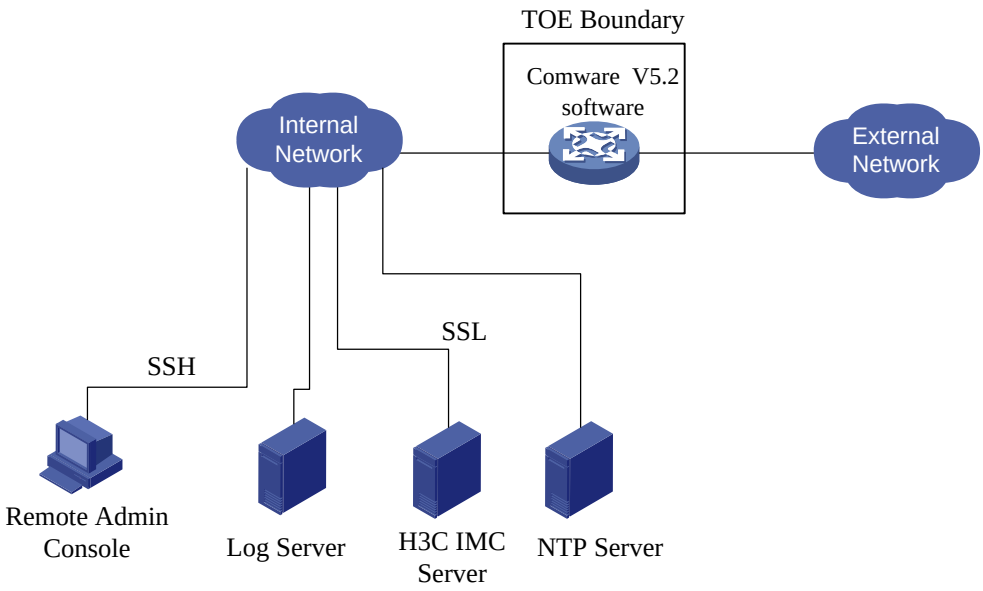
SR66 series routers: the SR66 series routers are intended to work as high-performance service gateways, distribution and access routers on industry networks, core, distribution, and access devices on large-sized networks, and core devices on small-/medium-sized enterprise networks.

SR88 series routers: the SR88 series routers are high-end routers intended to work at the core layer and distribution layer of large-sized IP MANs, core layer of dedicated industry networks, point of presence (POP), and distribution layer of carrier's networks.

All routers mentioned above run Comware V5.2.

1.4.1 Physical Boundaries

Figure 1-1 Physical environments and boundaries of the TOE



The TOE is the network Operating System software (NOS), Comware V5.2 release no. 1002(CC) running on MSR 20, MSR 30, MSR 50 , SR 66 and SR 88 series routers. The router hardware act as environment to the The operating environment of the TOE is the network where the TOE resides. In

Figure 1-1, HP iMC Server (the intelligent management center (iMC) developed by HP) functions as an AAA server to interoperate with the network devices to implement the AAA function. Additionally, an RFC 3164-compliant log server can be used for storing log files and an NTP server can be used as the time server for providing precise time for routers without hardware clocks.

To remotely manage the TOE, an administrator must use SSH to access it. The Remote Admin Console, Log Server, and iMC Server must be connected to the internal network.

1.4.2 Logical Boundaries

The TOE provides configuration and operations of the following security functions. Note that the log server function of SysLog Server, the AAA server function of the iMC Server, and the NTP server function are collaborating functions between the TOE and the IT-trusted products, and are considered IT environment functions. Therefore, the TSF does not contain the functions provided by the three servers.

- Audit

The TOE can generate various logs, such as TOE operation logs and event logs. The contents of the logs are compliant with RFC 3164. The audited events of the TOE include: administrative events, SSH access control events, and RADIUS authentication events. The TOE has compatibility with external syslog server for delivery of log messages as per RFC 3164. For the timestamp purpose the TOE has the capability to synchronize with remote NTP server.

- Identification and authentication

With the unified authentication mechanism provided by Comware V5.2, the TOE can identify and authenticate users. Comware V5.2 provides RADIUS and LOCAL authentication methods.

- Traffic filtering and routing

The TOE provides the access control list (ACL) function to check packets arriving at each interface and depending on the check results makes permit or deny decisions. An ACL allows the TOE to make access control based on packet information such as source and destination IP addresses, upper layer protocol fields (IP and ICMP), and other information.

The TOE forwards traffic to its destination based on the routing table. The routing table includes both entries generated with routing protocols and entries created manually. The TOE supports the routing protocols like RIP, OSPF and BGP.

- Access control/security management

Access control is to control access to the services provided by the TOE. Access control uses the identification and authentication function to authenticate users, uses the authorization mechanism to authorize access privileges, and uses the audit function to log user accesses.

The TOE provides the command line interface (CLI) for user account management (used for authentication and authorization), system time setting, and system shutdown and re-start. By providing the access control function for the system management services, the TOE ensures that the

functions are accessible only to users authorized with the appropriate management privileges, thus realizing secure management.

- TSF protection

The TOE uses the access control mechanism to protect various system-provisioned services, including TSF. Additionally, Comware V5.2 is not an open generic operating system. Only Comware itself can access the hardware resources such as memory and the operating system services. No third-party IT entities can use such resources.

At startup, the TOE performs integrity check for TSF-related data, such as the Comware executable file making sure that the stored TSF executable code has not been tampered.

TOE has the capability of supporting secured remote log-in through SSH v2. SSHv2 can be used to protect data exchanged between remote administrators and the TOE to prevent the user authentication information and operation information from being intercepted. SSHv2 uses AES or TDES for data encryption. The TOE has capability to generate RSA key for exchanging symmetric keys for a SSHv2 session.

2 CC Conformance

- The TOE is Common Criteria Version 3.1（ISO/IEC 15408:2006）Part 2 and Part 3 conformant at EAL2.
- The TOE does not conform to any Protection Profiles.
- The TOE does not use any packages.

3 Security Problem Definition

This section describes the TOE problem definition, including Threats, Assumptions, and organizational security policy (OSP).

3.1 Threats

The following table shows the threats related to the TOE and the IT environment. The threat agents are unauthorized users and unauthorized external IT entities.

Table 3-1 Threats

Threat code	Description
T.NOAUDIT	Administrative actions performed by users may not be known to the administrators due to actions not being recorded. The provided audit log format and audit log retrieval methods are inappropriate. The stored audit records may be modified or deleted by unauthorized users.
T.RES_EXP	An unauthorized entity may send impermissible information through the TOE which results in the exploitation of resources on the network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE to disrupt operations of the TOE.
T. DATA	An unauthorized user modifies or destroys TSF data on the TOE, which may cause the TOE to be inappropriately configured; A user may gain inappropriate access to the TOE by replaying authentication information (e.g., captured as transmitted during the course of legitimate use).
T.MANDAT	Unauthorized changes to the network configuration may be made through interception of in-band router/switch management traffic on a network.
T.NOMACT	An unauthorized user gains management access to the TOE and views or changes the TOE security configuration.
T.NOMGT	The administrator is not able to easily manage the security functions of the TOE, resulting in the potential for the TOE configuration to compromise security objectives and policies.
T.TIME	An authorized administrator will not be able to determine the sequence of events in the audit trail because the audit records are not correctly time-stamped.

3.2 Organizational Security Policies

There are no organizational security policies that the TOE must meet.

3.3 Assumptions

3.3.1 Personnel Assumptions

Table 3-2 Personnel assumptions

Assumption code	Description
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the

Assumption code	Description
	instructions provided by the TOE documentation, including the administrator guidance.
A.TRAIN_AUDIT	Administrators will be trained to periodically review audit logs to identify sources of concern.
A.TRAIN_GUIDAN	Administrators will be trained in the appropriate use of the TOE to ensure security.

3.3.2 Physical Assumptions

Table 3-3 Physical assumptions

Assumption code	Description
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.3.3 IT Environment Assumptions

Table 3-4 IT environment assumptions

Assumption code	Description
A.CONFIDENTIALITY	The hard copy documents that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to Authorized administrators.
A.GENPUR	There are no general-purpose computing capabilities (for example, the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.INTEROPERABILITY	The TOE will be able to function with the software and hardware of other vendors' routers/switches, and the Log Server, and iMC Server on the network. The Log Server, iMC Server and NTP Server should be connected in the internal trusted network.
A.LOWEXPT	The threat of malicious attacks aimed at exploiting the TOE is considered low.
A.SECSHELL	Administrators shall use SSH or SSL when remotely logging in to the TOE or external servers to access security-related information.
A.RADIUSMD5	When RADIUS is used for remote authentication, make sure that RADIUS has been implemented properly, and 128-bit MD5 protection is performed for the password.

Assumption code	Description
A.TIME	The NTP server in the network is available.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 4-1 TOE security objectives

Security objective code	Description
O.ACCESS_CONTROL	The TOE will restrict access to the TOE Management functions to the certain privileged level administrators.
O.I FC	The TOE must mediate the unauthenticated network traffic between source and destination network entities governed by the TOE.
O.AUDIT	Users must be accountable for their administrative actions on the TOE. The appropriate audit event log format is provided.
O.CFG_MANAGE	The TOE must provide services that allow effective management of its TSF and TSF-data.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access.
O.SELFPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. The protection involves Authentication data protection and TSF data protection.
O.TIME	The TOE provides a hardware clock and guarantees the time is precise.

4.2 Security Objectives for the Environment

Table 4-2 Environment security objectives

Security objective code	Description
OE.TRAIN_AUDIT	Administrators will be trained to periodically review the audit

Security objective code	Description
	logs to identify sources of concern.
OE.CONFIDENTIALITY	The hard copy documents that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to Authorized administrators.
OE.GENPUR	There are no general-purpose computing capabilities (for example, the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.INTEROPERABILITY	The TOE will be able to function with the software and hardware of other vendors, and the Log Server, iMC Server, and NTP Server on the network. The Log Server shall meet RFC3164. The Log Server shall provide the appropriate audit log format and log retrieval means. The Log Server, iMC Server and NTP Server should be connected in the internal trusted network.
OE.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
OE.LOWEXP	The threat of malicious attacks aimed at exploiting the TOE is considered low.
OE.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance.
OE.TRAIN_GUIDAN	Administrators will be trained in the appropriate use of the TOE to ensure security and will refer to all administrative guidance to ensure the correct operation of the TOE.
OE.USESECSHELL	Administrators use SSH or SSL for remote management.
OE.RADIUSMD5	RADIUS protocol uses the 128-bit MD5 to protect the authentication data and packet integrity.
OE.TIME	The NTP server can provide precise time.

5 Extended Component Definition

No extended components required for this ST as all requirements are drawn from Common Criteria Parts 2 and 3.

6 IT Security Requirements

6.1 Conventions

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

- Assignment: indicated with bold text
- Selection: indicated with underlined text
- Refinement: indicated with bold text and italics
- Iteration: indicated with typical CC requirement naming followed by a number in parentheses for each iteration (for example, FMT_CKM.1(1))

Additionally, four levels of user privilege are provided by the TOE: visit-user, monitor-user, config-user and manage-user. The term “user” is used when all for categories are included. All users are administrative users(namely administrator).

Table 6-1 User Roles

Level	Privilege(Roles)	Description
0	Visit	Involves commands for network diagnosis and commands for accessing an external device. Commands at this level are not allowed to be saved after being configured. After the device is restarted, the commands at this level will be restored to the default settings. Commands at this level include ping, tracert, and ssh2.
1	Monitor	Includes commands for system maintenance and service fault diagnosis. Commands at this level are not allowed to be saved after being configured. After the device is restarted, the commands at this level will be restored to the default settings. Commands at this level include debugging, terminal, refresh, reset, and send.
2	Config	Provides service configuration commands, including routing and commands at each level of the network for providing services. By default, commands at this level include all configuration commands except for those at manage level.
3	Manage	Influences the basic operation of the system and the system support modules for service support. By default, commands at this level involve file system, user management, level setting, as well as parameter setting within a system (the last case involves those non-protocol or non RFC provisioned commands).

6.2 Security Functional Requirements

This section describes the security SFRs from CC-part2 for the TOE. The components are listed in the following table, showing completed operations.

Table 6-2 SFRs list

Security Functional Class	Security Functional Components
Audit(FAU)	FAU_GEN.1.1
	FAU_GEN1.2
	FAU_GEN.2.1
	FAU_SAR.1.1
	FAU_SAR1.2
	FAU_STG.1.1
	FAU_STG.1.2
Cryptographic support(FCS)	FCS_CKM.1.1
	FCS_CKM.4.1
	FCS_COP.1.1
User Data Protection(FDP)	FDP_IFC.1.1
	FDP_IFF.1.2
	FDP_IFF.1.3
	FDP_IFF.1.4
	FDP_IFF.1.5
Identification and Authentication(FIA)	FIA_AFL1.1
	FIA_AFL1.2
	FIA_ATD.1.1
	FIA_UAU.2.1
	FIA_UID.2.1
Security Management(FMT)	FMT_MOF.1.1
	FMT_MTD.1.1
	FMT_SMF.1.1
	FMT_SMR.1.1
	FMT_SMR.1.2
TOE Access(FTA)	FTA_MCS.1.1
	FTA_MCS.1.2

Security Functional Class	Security Functional Components
	FTA_TSE.1.1
Protection of the TSF (FPT)	FPT_TST.1.1
	FPT_TST.1.2
	FPT_TST.1.3
	FPT_STM.1.1

6.2.2 Security Audit (FAU)

6.2.2.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

1) FAU_GEN.1.1

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

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

b) All auditable events for the [not specified] level of audit; [**specified in the table 6-3**]; and

c) [**Other specifically defined auditable events:**

1. **user login or logout**
2. **login failures; and**
3. **saving configuration**].

2) 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 (if applicable); and

b) For each audit event type, based on the auditable event, [**the information specified in the Additional Audit Record Contents column of the table 6-3**].

Table 6-3 Auditable event table

Functional component	Auditable event	Additional Audit Record Contents
FAU_SAR.1	Reading of information from the audit records.	User ID, and the command used for users to view the audit logs
FCS_CKM.1	Success and failure of the activity.	User ID, and the command used for users to create keys
FCS_CKM.4	Success and failure of the activity.	User ID, and the command used for users to destroy keys
FCS_COP.1	Success and failure, and the type of cryptographic operation.	User ID
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	USER ID
FIA_UAU.2	All use of the authentication mechanism.	User ID
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	User ID
FMT_MOF.1	All modifications in the behavior of the functions in the TSF.	User ID, and the command used for modifying the behavior of the functions in the TSF.
FMT_MTD.1	All modifications to the values of TSF data.	User ID, and the command used for modifying TSF data
FMT_SMF.1	Use of the management functions	User ID, and the commands corresponding to the management functions
FMT_SMR.1	modifications to the group of users that are part of a role;	User ID, and the command used for modifying the roles (privilege levels)
FPT_STM.1	changes to the time	User ID, and the command used for modifying time
FPT_TST.1	Execution of the TSF self tests and the results of the tests.	None
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions.	User ID
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	User ID

6.2.2.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

1) 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.

6.2.2.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

1) FAU_SAR.1.1

The TSF shall provide [**monitor-user, config-user, manage-user**] with the capability to read [**all audit trail data**] from the audit records.

2) FAU_SAR.1.2

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

6.2.2.4 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

1) FAU_STG.1.1

The TOE shall protect the stored audit records from unauthorized deletion.

2) FAU_STG.1.2

The TOE shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

6.2.3 Cryptographic support (FCS)

6.2.3.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies:

- [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
- FCS_CKM.4 Cryptographic key destruction

1) FCS_CKM.1.1 –RSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA**] and specified cryptographic key sizes [**512, 1024, and 2048 bits**] that meet the following: [**PKCS #1**].

6.2.3.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes,
- or FDP_ITC.2 Import of user data with security attributes,
- or FCS_CKM.1 Cryptographic key generation]

1) FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwrite**] that meets the following: [**none**]

6.2.3.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes,
- or FDP_ITC.2 Import of user data with security attributes,
- or FCS_CKM.1 Cryptographic key generation]
- FCS_CKM.4 Cryptographic key destruction

1) FCS_COP.1.1–Remote Administration (SSH2)

The TSF shall perform [**encryption of remote authorized administrator sessions**] in accordance with a specified cryptographic algorithm [**3DES as specified in FIPS PUB 46-3 and implementing any mode(CBC-I ,CFB -1bit, CFB-8 bit, CFB-P-1bit, CFB-P-8bit, CFB-P 64bit, OFB-I modes are not supported) of operation specified in FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys) or Advanced Encryption Standard (AES) as specified in FIPS PUB 197(CFB1 , CFB8 modes are not supported)**] and cryptographic key sizes [**that are 168 binary digits of 3DES and 128 binary digits of AES]** that meet the following: [**FIPS PUB 46-3 with Keying Option 1 or FIPS 197**.]

6.2.4 User data protection

6.2.4.1 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

1) FDP_IFC.1.1

The TSF shall enforce the [UNAUTHENTICATED SFP] on

a) [subjects**:**

- **unauthenticated external IT entities that send and receive packets through the TOE to one another;**

b) information (packets):

- **network packets sent through the TOE from one subject to another;**

c) operation:

- **route packets.**]

6.2.4.2 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies:

- FDP_IFC.1 Subset information flow control
- FMT_MSA.3 Static attribute initialization

1) FDP_IFF.1.1

The TSF shall enforce the [UNAUTHENTICATION SFP] based on the following types of subject and information security attributes: [

a) subject security attributes:

- **presumed address**

b) information security attributes:

- **presumed address of source subject**
- **presumed address of destination subject**
- **network layer protocol (IP, ICMP)**
- **TOE interface on which packet arrives and departs**

2) 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: [

subjects on a network can cause packets to flow through the TOE to another connected network if:

- **all the packet 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 packet security attributes, created by the authorized user;**
- **the presumed address of the source subject, in the packet, is consistent with the network interface it arrives on;**
- **and the presumed address of the destination subject, in the packet, can be mapped to a configured nexthop.**]

3) FDP_IFF.1.3

The TSF shall enforce the [**no additional UNAUTHENTICATED SFP rules**].

4) FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [**no additional rules that explicitly authorize information flows**]

5) FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [**no additional rules that explicitly deny information flows**].

6.2.5 Identification and Authentication (FIA)

6.2.5.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

1) FIA_AFL.1.1

The TSF shall detect when [an administrator configurable positive integer within **1-5**] unsuccessful authentication attempts occur related to [**login**].

2) 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 administrator or locking period expired**].

6.2.5.2 FIA_ATD.1 User Attribute Definition

Hierarchical to: No other components.

Dependencies: No dependencies.

1) FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

[**a) identity;**

b) authentication data (for example, password);]

6.2.5.3 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

1) 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.

6.2.5.4 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

1) 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.

6.2.6 Security Management (FMT)

6.2.6.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

1) FMT_MOF.1.1

The TSF shall restrict the ability to [determine the behavior of] the functions **listed below** to [the **manage-user or config-user or monitor-user or visit-user**]:

privilege level	management operations
visit	• change privilege level; • reset and change visit-user himself password;
monitor	• change privilege level; • review the audit trail; • reset and change of monitor-user himself password;
Config	• change privilege level; • save configuration; • review the audit trail; • management of the information center; • start-up and shut-down the audit functions; • management of the logbuffer; • management of the logfile; • change the log output destination; • maintenance of config-user himself password; • maintenance of the super password; • maintenance(create, destroy, import, export) public key; • managing(create, modify, delete, apply) the filtering rules; • management of firewall;
Manage	• change privilege level; • save configuration;

privilege level	management operations
	• review the audit trail; • management of the information center; • start-up and shut-down the audit functions; • management of the logbuffer; • management of the logfile; • change the log output destination; • maintenance of manage-user himself password; • reset the password of lower level user; • maintenance of the super password; • maintenance(create, destroy, import, export) public key; • managing (create, modify, delete, apply) the filtering rules; • management of firewall; • reboot TOE; • maintenance (delete, modify, add) of the group of users with read access right to the audit records; • management of the threshold for unsuccessful authentication attempts; • the management of the user identities; • managing the group of roles that can interact with the TSF data; • managing the group of users that are part of a role; • management of the time; • management of the maximum allowed number of concurrent user sessions by an administrator; • management of the session establishment conditions by the authorized administrator; • maintenance (delete) audit trail; • management of the RADIUS scheme; • maintenance (create, delete, modify) user account; • maintenance (delete, modify) system start-up parameters; • file operation (copy, delete, fixdisk, format, mkdir, move, rename, reset recycle-bin, rmdir, undelete); • management of the command privilege; • management of the terminal parameter; • management of SSH Server; • management of SFTP Server; • management of the ISP domain; • start-up and shut-down RADIUS client;

6.2.6.2 FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

1) FMT_MTD.1.1

The TSF shall restrict the ability to [modify or delete]TSF data [**listed below**] to [**manage-user or config-user**]:[

a) user account attributes;(manage-user, or config-user who can only delete/modify himself password)

b) Access control scheme: access method scheme, AAA scheme;(manage-user only)

c) audit logs(manage-user only)

d) system start-up parameters: configuration file, Comware image, boot ROM image; (manage-user only)

e) filtering rules (manage-user or config-user)

f) public key (manage-user or config-user)

g) clock (manage-user only)

6.2.6.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

1) FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:[

a) change privilege level;

b) save configuration;

c) review the audit trail;

d) management of the information center;

e) start-up and shut-down the audit functions;

f) management of the logbuffer;

g) management of the logfile;

h) change the log output destination;

i) maintenance of manage-user himself password;

j) reset the password of lower level user;

k) maintenance of the super password;

l) maintenance(create, destroy, import, export) public key;

m) managing (create, modify, delete, apply) the filtering rules;

n) management of firewall;

o) reboot TOE;

p) maintenance (delete, modify, add) of the group of users with read access right to the audit records;

q) management of the threshold for unsuccessful authentication attempts;

r) the management of the user identities;

s) managing the group of roles that can interact with the TSF data;

t) managing the group of users that are part of a role;

u) management of the time;

v) management of the maximum allowed number of concurrent user sessions by an administrator;

w) management of the session establishment conditions by the authorized administrator;

x) maintenance (delete) audit trail;

y) management of the RADIUS scheme;

z) maintenance (create, delete, modify) user account;

aa) maintenance (delete, modify) system start-up parameters;

bb) file operation (copy, delete, fixdisk, format, mkdir, move, rename, reset recycle-bin, rmdir, undelete);

cc) management of the command privilege;

dd) management of the terminal parameter;

ee) management of SSH Server;

ff) management of SFTP Server;

gg) management of the ISP domain;

hh) start-up and shut-down RADIUS client;

ii)]

6.2.6.4 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

1) FMT_SMR.1.1

The TSF shall maintain the roles:[**visit-user, monitor-user, config-user, manage-user**].

2) FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_MCS.1 Basic limitation on multiple concurrent sessions

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

1) FTA_MCS.1.1

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

2) FTA_MCS.1.2

The TSF shall enforce, by default, a limit of [**1024**] session per user.

6.2.7.2 FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

1) FTA_TSE.1.1

The TSF shall be able to deny session establishment based on [**user IP**].

6.2.8 Protection of the TSF (FPT)

6.2.8.1 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

1) FPT_TST.1.1

The TSF shall run a suite of self tests [during initial start-up] to demonstrate the correct operation of the [**parts of TSF listed bellow**]:

- **the security assumptions that underlies the TSF**

2) FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of [**parts of TSF data listed bellow**].

- **Comware executable file**

3) FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

6.2.8.2 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

1) FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

6.3 Security Assurance Requirements

The security assurance requirements for the ST are drawn from Common Criteria Part 3. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) as defined by the CC.The security assurance components are as follows:

Table 6-4 SARs list

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
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

Assurance Class	Assurance components
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

7.1 TOE Security Functions

7.1.1 Audit

The TOE is capable of basic data logging and security auditing. Audit data is stored in persistent memory on the Log Server. The Log Server is not a part of the TOE, but considered as a server of sound security measures, on which access to the audit data is under control.

Additionally, the TOE provides the local log buffer and log file function, which allows the administrator(all roles but the visit-user) to view recent logs for the current device at the CLI. The log buffer is located in the random access memory (RAM). The log file is located in the persistent memory on the TOE.

7.1.1.1 Audit data generation: FAU_GEN.1, FAU_GEN.2

Audit data is generated by HP Comware. Audit data includes audit records for the auditable events specified as follows **the table 6-3**.

Audit data is generated in an appropriate format that meets RFC3164. Audit data can be configured to store audit logs on the Log Server , log buffer and log file. Only the manage-user and config-user can change the output destination (e.g. a log server or the log buffer) of audit logs.

If available, the user that caused an audit event will be identified.

7.1.1.2 The time stamp for audit logs can be configured by manage-user and config-user.Security Audit review and restricted review: FAU_SAR.1, FAU_STG.1

The TOE provides the local log function including local log buffer and local log file function. The TOE provides authorized administrators the ability to read audit data on the TOE.

The TOE provides the ability for authorized administrators(manage-user only)to delete audit data on the TOE..

Commands are available to display the entire log buffer/file, or to select records that match or do not match a pattern.

The log buffer on the TOE has capacity limitations. When the log buffer size reaches the maximum, new logs will overwrite the old ones. The administrator(manage-user and config-user) can set the maximum log buffer size, which is up to 1024 log entries.

The log file on TOE has capacity limitations. When the size of a log file reaches the maximum, the earliest records will be deleted and new records will be writed into the log file. The directory for a log file varies with device models. Typically, a log file is saved in the directory /logfile/. To use the Log Server, which is not in the boundaries of the TOE, make sure that it provides the following abilities:

a. The Log Server shall protect the stored audit records in the audit trail from unauthorized deletion.
b. The Log Server shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

Additionally, the Log Server shall provide the following abilities:

a. The Log Server shall provide the manage-user the capability to read all information from the audit records.
b. The Log Server shall provide the audit records in a manner suitable for the user to interpret the information.

7.1.1.3 Reliable Time Stamps: FPT_STM.1

The TOE provides reliable time stamps for use by the hardware clocks of the TOE.

If an NTP server is used, make sure that it can provide precise time.

7.1.2 Traffic Filtering and Routing

7.1.2.1 Information Flow and Security Attributes: FDP_IFC.1, FDP_IFF.1

The TOE supports routing of the traffic that is permitted by the information flow policies. All traffic passing through the TOE is processed by the ACL attached to the interface. The ACL is processed top-down, with processing continuing until the first match is made. All traffic that successfully clears the ACLs is processed by the routing tables. The routing table is processed top-down, with processing

continuing until the first match is made. The routing table may be statically updated by a privileged administrator or dynamically through routing protocols.

7.1.3 Identification & Authentication

Identification and Authentication for logins to the TOE can be provided either locally on the TOE or remotely through the HP iMC Server. Authorized administrators (all roles) of the TOE must be identified and authenticated before using the system.

Local authentication with SSH2 utilizes the user's public key stored on the appliance for both establishing the SSH2 session and authenticating the user to the CLI.

7.1.3.1 User attribute definition: FIA_ATD.1

The user security attributes are identity and authentication data (passwords and public keys).

7.1.3.2 Identification and authentication: FIA_UAU.2, FIA_UID.2

Whichever access method is used for management sessions, successful authentication is required prior to giving a user access to the system. For example, it is possible for the mange-user to log in to the TOE by directly connecting to the console port. Administrators log in to perform local maintenance, diagnostics, or debugging. They must undergo identification and authentication before they can perform any other actions.

7.1.3.3 Failure handling: FIA_AFL.1

The TOE will terminate the access session and lock the user account after consecutive failed authentication attempts met an administrator configurable positive integer in the range **1** to **5**. The user account will be locked for a period, which is configurable in the range of 10 to 120 minutes. During this period, all accesses with the account will be rejected. When this period expires, the account will unlock automatically or be manually unlocked by the administrator.

7.1.4 Security Management

7.1.4.1 Management and specification of security functions and TSF data: FMT_MOF.1, FMT_SMF.1 and FMT_MTD.1

The TOE provides CLI for users to operate the device. The TOE divides all commands into four privilege levels, including visit, monitor, config, and manage. The levels here are consistent with the management privilege levels of users, and the users at a corresponding level can execute all commands at the same level or any lower level.

The following table shows the TSF-related and TSF-data-related management functions that users at a certain level can execute:

Table 7-1 Mapping of privilege with management operations

privilege level	management operations
visit	• change privilege level; • reset and change visit-user himself password;
monitor	• change privilege level; • review the audit trail; • reset and change of monitor-user himself password;
Config	• change privilege level; • save configuration; • review the audit trail; • management of the information center; • start-up and shut-down the audit functions; • management of the logbuffer; • management of the logfile; • change the log output destination; • maintenance of config-user himself password; • maintenance of the super password; • maintenance(create, destroy, import, export) public key; • managing(create, modify, delete, apply) the filtering rules; • management of firewall;
Manage	• change privilege level; • save configuration; • review the audit trail; • management of the information center; • start-up and shut-down the audit functions; • management of the logbuffer; • management of the logfile; • change the log output destination; • maintenance of manage-user himself password; • reset the password of lower level user; • maintenance of the super password; • maintenance(create, destroy, import, export) public key; • managing (create, modify, delete, apply) the filtering rules; • management of firewall; • reboot TOE; • maintenance (delete, modify, add) of the group of users with read access right to the audit records; • management of the threshold for unsuccessful authentication attempts; • the management of the user identities;

privilege level	management operations
	• managing the group of roles that can interact with the TSF data; • managing the group of users that are part of a role; • management of the time; • management of the maximum allowed number of concurrent user sessions by an administrator; • management of the session establishment conditions by the authorized administrator; • maintenance (delete) audit trail; • management of the RADIUS scheme; • maintenance (create, delete, modify) user account; • maintenance (delete, modify) system start-up parameters; • file operation; • management of the command privilege; • management of the terminal parameter; • management of SSH Server; • management of SFTP Server; • management of the ISP domain; • start-up and shut-down RADIUS client;

7.1.4.2 Security Roles: FMT_SMR.1

The TOE maintains the roles of four privilege levels, namely, visit, monitor, config, and manage.

The TOE can and shall be configured to authenticate and authorize unprivileged user as a certain privilege level to the CLI by using identity and authentication data.

7.1.5 Access Control

7.1.5.1 Basic limitation on multiple concurrent sessions: FTA_MCS.1

The maximum number of concurrent sessions can be set for each individual user. The default maximum number of concurrent sessions is **1024** when a new user created on the TOE.

7.1.5.2 TOE session establishment: FTA_TSE.1

The TOE is able to deny session establishment based on user IP, a session security attribute. The administrator can specify which attributes are to be bound when authenticating a user, and if the binding failed, the session establishment will be denied.

7.1.6 Protection of the TSF

7.1.6.1 System Start-up Self Checking: FPT_TST.1.1, FPT_TST.1.2, FPT_TST.1.3

At startup the TOE performs the integrity checking of comware executable file by CRC or MD5 to ensure the correct operation of the security assumptions that underlies the TSF **[** FPT_TST.1.1**].**

During the startup of the system, the user can press **CTRL+B** to access the Boot ROM operation menu to download the Comware executable file. In this case, the TOE automatically checks the file for integrity errors. [FPT_TST.1.2, FPT_TST.1.3]

7.1.6.2 Reliable Time Stamps: FPT_STM.1

The hardware clock provides reliable time stamps for use by the components of the TOE.

If an NTP server used, the date/time will be obtained by the NTP protocol and set automatically.

7.1.6.3 Remote Management: FCS_COP.1, FCS_CKM.1, FCS_CKM.4

The TOE implements Secure Shell version 2 (SSHv2) with RSA key generation and 168-bit 3DES or 128-bit AES encryption for remote management.

Key overwriting is done when new cryptographic keys are created, and the new key overwrites the old one in the NVRAM.

The implementation of SSHv2 provides an integrated single use mechanism where the transport protocol provides a unique session identifier bound to the key exchange process. The identifier is used by higher level protocols to bind data to a given session and prevent replay of data from prior sessions.

Remote management of the router via SSHv2 provides full access to the CLI command set.

With the support for the various cryptographic standards, the TOE ensures that only appropriate secure values are used for the cryptographic functions that are performed.

7.2 Security Assurance Measures

Table 7-2 Security assurance measures

Assurance Requirements	Assurance Components
ADV_ARC.1	The Security architecture description is provided in Comware High Level Design
ADV_FSP.2	The Security-enforcing functional specification is provided in Comware Functional Specification
ADV_TDS.1	The security architecture description is provided in Comware High Level Design

Assurance Requirements	Assurance Components
AGD_OPE.1	The operational user guidance is provided in Operation Manual and Command Manual
AGD_PRE.1	The preparative procedures is provided in Installation Manual
ALC_CMC.2	The use of CM system is provided in Configuration Management Procedure
ALC_CMS.2	The parts of the TOE CM coverage is provided in Configuration Management Plan
ALC_DEL.1	The delivery procedures is provided in Delivery Procedure
ASE_CCL.1	The conformance claims is provided in this ST
ASE_ECD.1	The extended components definition is provided in this ST
ASE_INT.1	The ST introduction is provided in this ST
ASE_OBJ.2	The security objectives is provided in this ST
ASE_REQ.2	The derived security requirements is provided in this ST
ASE_SPD.1	The security problem definition is provided in this ST
ASE_TSS.1	TOE summary specification is provided in this ST
ATE_COV.1	The evidence of coverage is provided in Test Plan
ATE_FUN.1	The functional testing description is provided in Test Plan
ATE_IND.2	The testing – sample is provided in Test Plan and Test Cases
AVA_VAN.2	Refer to AGD_PRE.1 and AGE_OPE.1

8 Rationale

8.1 Rationale for Security Objectives

8.1.1 Rationale for Security Objectives for the TOE

Table 8-1 Security objectives to threats mapping

	T.DATA	T.MANDAT	T.NOAUDIT	T.NOAUTH	T.NOMACT	T.RES_EXP	T.NOMGT	T.TIME
O.ACCESS_CONTROL	X				X			
O.IFC						X		
O.AUDIT			X					
O.CFG_MANAGE							X	
O.IDAUTH					X			
O.SELFPRO	X	X		X				
O.TIME								X

T. DATA: To deal with the T.DATA threat, the O.ACCESS_CONTROL security objective is necessary because it allows only administrators with the appropriate privilege to access, modify, or delete the TSF-Data of audit logs, configuration files, and key files stored on the TOE. The O.SELFPRO security objective is necessary because it protect the integrity of the authentication data to avoid that a user may gain inappropriate access to the TOE by replaying authentication information. The O.SELFPRO protect the integrity of TSF data to avoid that TOE may be inappropriately configured by tampering TSF data.

T.MANDAT: To deal with the T.MANDAT threat, the O.SELFPRO security objective is necessary because the objective can protect remote management information and authentication data from being intercepted by requiring the use of SSH to provide secure encrypted sessions.

T.NOAUDIT: To deal with the T.NOAUDIT threat, the O.AUDIT security objective is necessary because it requires the use of logging function to create audit records of user's administrative actions on the TOE. In addition, the appropriate audit log format and log retrieval means are necessary.

Finally, The O.AUDIT can protect the audit trail storatge from unauthorized modifications or deletion.

T.NOAUTH: To deal with the T.NOAUTH, The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

T.NOMACT: To deal with the T.NOMACT threat, the O.IDAUTH is necessary because it requires that every user undergo identity verification and authentication before it can be authorized access to the TOE management service. In addition, the O.ACCESS_CONTROL security objective is necessary because it requires access control for the system management service to ensure that only administrators with appropriate privileges can access the security management function or security-related data.

T.RES_EXP: To deal with the T.RES_EXP threat, the O.IFC security objective requires that all information that passes through the network is mediated and governed by the TOE.

T.NOMGT: To deal with the T.NOMGT threat, the O.CFG_MANAGE security objective is necessary because it requires provision of management tools/applications for administrators to manage security functions, reducing the possibility for error.

T.TIME: To deal with the T.TIME threat, the O.TIME security objective is necessary because it requires the TOE to provide precise time service to guarantee that the timestamp of the audit logs is in order.

8.1.2 Rationale for Security Objectives for the Environment

Table 8-2 Environment security objectives to assumptions mappings

	T.NOAUDIT	A.NOEVIL	A.TRAIN_AUDIT	A.TRAIN_GUIDAN	A.LOCATE	A.CONFIDENTIALITY	A.GENPUR	A.INTEROPERABILITY	A.LOWEXPT	A.SECSHELL	A.RADIUSMD5	A.TIME
OE.TRAIN_AUDIT			X									
OE.CONFIDENTIALITY	X					X						
OE.GENPUR							X					
OE.INTEROPERABILITY	X							X				
OE.LOCATE					X							
OE.LOWEXP									X			
OE.NOEVIL		X										

	T.NOAUDIT	A.NOEVIL	A.TRAIN_AUDIT	A.TRAIN_GUIDAN	A.LOCATE	A.CONFIDENTIALITY	A.GENPUR	A.INTEROPERABILITY	A.LOWEXPT	A.SECSHELL	A.RADIUSMD5	A.TIME
OE.USESECSHELL										X		
OE.RADIUSMD5											X	
OE.TRAIN_GUIDAN				X								
OE.TIME												X

T.NOAUDIT: To counter the threat of T.NOAUDIT to the audit logs stored on the Log Server, the OE.CONFIDENTIALITY and OE.INTEROPERABILITY objectives are necessary. The OE.CONFIDENTIALITY requires that only authorized user can access the audit logs stored on the Log Server, which protects the audit logs against unauthorized review, deletion or modification. The OE.INTEROPERABILITY requires that the Log Server should meet RFC3164 to receive the audit data generated by the TOE. The OE.INTEROPERABILITY also requires the appropriate audit log format and log retrieval means. Finally, the OE.INTEROPERABILITY requires that the Log Server should be connected to the trustworthy network, which prevents the packets of audit logs from being intercepted.

A.NOEVIL: To ensure the effectiveness of the A.NOEVIL assumption, the OE.NOEVIL objective is necessary because it requires that the authorized administrators be not careless, willfully negligent, or hostile, and follow and abide by the instructions provided by the TOE documentation. Nevertheless, authorized administrators are capable of error.

A.TRAIN_AUDIT: To ensure the effectiveness of the A.TRAIN_AUDIT assumption, the OE.TRAIN_AUDIT objective is necessary because it requires that the administrators be trained to periodically check the audit logs to identify log sources of concern.

A.TRAIN_GUIDAN: To ensure the effectiveness of the A.TRAIN_GUIDAN assumption, the OE.TRAIN_GUIDAN objective is necessary because it requires that the administrators be trained to operate the TOE correctly following the management guidance.

A.LOCATE: To ensure the effectiveness of the A.LOCATE assumption, the OE.LOCATE objective is necessary because it requires that the processing resources of the TOE be located within the access control facilities, which will prevent unauthorized physical access.

A.CONFIDENTIALITY: To ensure the effectiveness of the A.CONFIDENTIALITY assumption, the OE.CONFIDENTIALITY objective is necessary because it requires that the external hard copy of the

configuration file, identification and authentication information, audit logs, and key files be kept confidential and only the authorized administrators can access them.

A.GENPUR: To ensure the effectiveness of the A.GENPUR assumption, the OE.GENPUR objective is necessary because it requires that the TOE should not provide general-purpose computing and storage capabilities.

A.INTEROPERABILITY: To ensure the effectiveness of the A.INTEROPERABILITY assumption, the OE.INTEROPERABILITY objective is necessary because it requires that the TOE be able to interoperate with the external NTP Server, iMC Server, and network devices of other vendors.

A.LOWEXPT: To ensure the effectiveness of the A.LOWEXPT assumption, the OE.LOWEXP objective is necessary because it requires that the threat of malicious attacks by exploiting the TOE be considered low.

A.SECSHELL: To ensure the effectiveness of the A.SECSHELL assumption, the OE.USESECSHELL objective is necessary because it requires that the administrators use SSH or SSL to remotely manage the TOE or other external servers.

A.RADIUSMD5: To ensure the effectiveness of the A.RADIUSMD5, the OE.RADIUSMD5 objective is necessary because it requires that RADIUS protocol uses the 128-bit MD5 to protect the authentication data and packet integrity.

A.TIME: To ensure the effectiveness of the A.TIME assumption, the OE.TIME objective is necessary because it requires that the external NTP server provide precise time services.

8.2 Rationale for Security Requirements

8.2.1 Rationale for TOE security functional requirements

Table 8-3 SFRs to security objectives mappings

	O.ACCESS_CONTROL	O.AUDIT	O.CFG_MANAGE	O.IDAUTH	O.IFC	O.SELFPRO	O.TIME
FAU_GEN.1		**X**					
FAU_GEN.2		**X**					
FAU_SAR.1		**X**					
FAU_STG.1		**X**					

	O.ACCESS_CONTROL	O.AUDIT	O.CFG_MANAGE	O.IDAUTH	O.IFC	O.SELFPRO	O.TIME
FCS_CKM.1						X	
FCS_CKM.4						X	
FCS_COP.1						X	
FDP_IFC.1					X	X	
FDP_IFF.1					X	X	
FIA_AFL.1				X			
FIA_ATD.1	X	X		X			
FIA_UAU.2				X			
FIA_UID.2				X			
FMT_MOF.1	X		X			X	
FMT_MTD.1	X		X			X	
FMT_SMF.1			X				
FMT_SMR.1	X		X			X	
FTA_MCS.1	X						
FTA_TSE.1	X						
FPT_TST.1						X	
FPT_STM.1		X					X

8.2.1.2 O.ACCESS_CONTROL

To ensure that all the accesses to TOE security functions and configuration data are controlled, the FIA_ATD.1 component and the FMT_SMR.1 component are used for recognizing the user and the associated administrative role that exists for the TOE, the FMT_MOF.1 component provides the ability to restrict the use of TOE security functions to authorized administrators of the TOE, and the FMT_MTD.1 component ensures that only authorized administrators of the TOE can modify TOE data.

The FTA_TSE.1 component is used to ensure that the TOE is able to deny session establishment based on attributes such as originating location (IP, for example).

The FTA_MCS.1 component is used to restrict the maximum number of concurrent sessions associated with the same user for efficient use of the resources of the TOE, and by default, a limit of 1 session per user is adopted.

8.2.1.3 O.AUDIT

To generate audit records which will include the time that the event occurred and if applicable, the identity of the user performing the event, the FIA_ATD.1 component is used to maintain security attributes belonging to individual users, the FAU_GEN.1 and FAU_GEN.2 components are used to ensure that security relevant events are defined and auditable for the TOE, and the FPT_STM.1 component is used to ensures that the timestamps associated with the audit records are reliable.

The FAU_SAR.1 component is used to provide the capability to review Audit data and ensure that security relevant events are available for review by authorized administrators. The FAU_STG.1 component is used to protect audit data from unauthorized modifications or deletion.

8.2.1.4 O.CFG_MANAGE

The FMT_MOF.1 component is used to provide management tools such as the CLI to allow authorized administrators to manage and perform security functions.

The FMT_SMF.1 component is used to ensure that the TOE is capable of performing numerous management functions including startup, shutdown, and creating/modifying/deleting configuration items. The FMT_SMR.1 component is used to manage the administrative roles that exist for the TOE.

The FMT_MTD.1 component is used to ensure that only the super user of the TOE may modify TSF data. The TOE requires that all entities' actions resulting in the access to TOE security functions and configuration data are controlled to prevent unauthorized activity.

The TOE ensures that access to TOE security functions and configuration data is done in accordance with the rules of the access control policy.

8.2.1.5 O.IDAUTH

The TOE must uniquely identify and authenticate the claimed identity of users before granting management access.

The FIA_ATD.1 component is used to provide users with security attributes to enforce the authentication policy of the TOE and to associate security attributes with users. The FIA_UID.2 and FIA_UAU.2 components are used to ensure that users authorized to access the TOE are defined using identification and authentication. The FIA_UID.2 component is used to ensure that before anything occurs on behalf of a user, the user's identity is identified to the TOE.

The FIA_AFL.1 components ensure that multiple consecutive unsuccessful attempts to authenticate result in termination of the session establishment process.

8.2.1.6 O.IFC

The TOE is required to identify the entities involved in the unauthenticated information flow control SFP [FDP_IFC.1] and to identify the attributes of the users sending and receiving the information in the unauthenticated SFP [FDP_IFF.1]. The policy is defined by saying under what conditions information is permitted to flow [FDP_IFF.1]. Information that is permitted to flow will then be routed according to the information in the routing table [FDP_IFF.1].

8.2.1.7 O.SELFPRO

The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. To achieve this, The FCS_COP.1, FCS_CKM.1, and FCS_CKM.4 components are used to provide an encrypted (SSHv2) mechanism for remote management of the TOE. The TOE ensures that the TSF has a domain of execution that is separate and that cannot be violated by unauthorized users.

The three components FMT_SMR.1, FMT_MOF.1, and FMT_MTD.1 guarantee that only users with the corresponding privilege can modify the system startup parameters and the TSF data, so that illegal users cannot bypass the security function to get the operation right of the TOE. The

The two components FDP_IFC.1 and FDP_IFF.1 guarantee that only information streams conforming to certain rules can be processed and forwarded, so that the TOE resources will not be over-occupied by illegal information streams, which may make the functions unavailable.

The TOE will perform initial startup tests upon bootup of the system. The TOE is required to demonstrate the correct operation of the security assumptions that underlies the TSF. The TOE provide authorized users with the capability to verify the integrity of parts of TSF data and stored TSF executable code[FPT_TST.1].

8.2.1.8 O.TIME

The FPT_STM.1 component is used to provide reliable time stamps for the TSFs of the TOE, for example, audit record generation.

8.2.2 Rationale for TOE Environment Security Functional Requirements

Table 8-4 Environment security functional requirements

OE.CONFIDENTIALITY	The Log Server is used to store logs, the logs must be kept confidential and only accessible to authorized administrators. When an iMC server is used to authenticate the users, the user authentication information on it must be kept confidential and only accessible to authorized administrators. The manage user must guarantee the security of the configuration file, ensuring that it cannot be tampered.

OE.INTEROPERABILITY	The Log Server is used to store logs. It must meet RFC3164, and must provide an appropriate audit log format and log retrieval means.
OE.TIME	If an NTP server is used, make sure that the NTP server can provide precise time.

8.2.3 Dependencies Rationale

All functional and assurance requirements dependencies indicated in [CC2] and [CC3] have been satisfied.

Table 8-5 SFRs dependencies

Functional component	Dependencies
FAU_GEN.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1,FIA_UID.1
FAU_SAR.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1
FCS_CKM.1	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	FCS_CKM.1
FCS_COP.1	FCS_CKM.1,FCS_CKM.4
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1
FIA_AFL.1	FIA_UAU.1, via FIA_UAU.2
FIA_ATD.1	None
FIA_UAU.2	FIA_UID.1, via FIA_UID.2
FIA_UID.2	None
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	None
FMT_SMR.1	FIA_UID.1
FTA_MCS.1	FIA_UID.1
FTA_TSE.1	None
FPT_TST.1	None
FPT_STM.1	None

8.3 TOE Summary Specification Rationale

Table 8-6 SFRs to summary specifications mappings

	Audit	Identification & Authentication	Traffic Filtering and Routing	Security Management	Access Control	Protection of the TSF
FAU_GEN.1	X					
FAU_GEN.2	X					
FAU_SAR.1	X					
FAU_STG.1	X					
FCS_CKM.1						X
FCS_CKM.4						X
FCS_COP.1						X
FDP_IFC.1			X			X
FDP_IFF.1			X			X
FIA_AFL.1		X				
FIA_ATD.1		X				
FIA_UAU.2		X				
FIA_UID.2		X				
FMT_MOF.1				X		X
FMT_MTD.1				X		X
FMT_SMF.1				X		
FMT_SMR.1				X		X
FTA_MCS.1					X	
FTA_TSE.1					X	
FPT_TST.1						X
FPT_STM.1	X					X

8.4 Security Assurance Measures & Rationale

Table 8-7 Security assurance measures & rationale

Assurance Requirements	Assurance Measures	Assurance Rationale
ADV_ARC.1	Comware High Level Design	Provides the security architecture description of the security domains maintained by the TSF that are consistent with the SFRs. Since self-protection is a property of the TSF that is achieved through the design of the TOE and TSF, and enforced by the correct implementation of that design, self-protection will be achieved by that design and implementation.
ADV_FSP.2	Comware Functional Specification	The informal functional specification document identifies the interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.
ADV_TDS.1	Comware High Level Design	The security enforcing high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.
AGD_OPE.1	Operation Manual Command Manual	Provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE, security parameters that are configurable by the administrator, how to configure the TOE's rule set and the implications of any dependencies of individual rules. The documentation also provides a description of how to setup and review the auditing features of the TOE.
AGD_PRE.1	Installation Manual	Ensures the administrator has the information necessary to install the TOE in the evaluated configuration. The Installation, Generation and Startup documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration.
ALC_CMC.2	Configuration Management Procedure	A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labeling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Assurance Requirements	Assurance Measures	Assurance Rationale
ALC_CMS.2	Configuration Management Plan	Placing the TOE itself, the parts that comprise the TOE, and the evaluation evidence required by the other SARs under CM provides assurance that they have been modified in a controlled manner with proper authorizations.
ALC_DEL.1	Delivery Procedure	Provided documentation that instructs how to ensure the delivery of the TOE, in whole or in parts, has not been tampered with or corrupted during delivery. This requirement ensures the administrator has the ability to begin their TOE installation with a clean (for example, malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE.
ATE_COV.1	Comware V5.2 Test Plan	The test coverage document provides a mapping of the test cases performed against the TSF. Establishes that the TSF has been tested against its functional specification.
ATE_FUN.1	Comware V5.2 Test Plan	Provides the necessary test documentation to allow for an independent analysis of the developer's security functional test coverage. In addition, it provides the test suite executables, which are used for independently verifying the test suite results and in support of the test coverage analysis activities.
ATE_IND.2	Comware V5.2 Test Plan Comware V5.2 Test Cases	Independent confirmation of the developer's test results, by mandating a subset of the test suite be run by an independent party. This component also requires an independent party to attempt to craft functional tests that address functional behavior that is not demonstrated in the developer's test suite. Upon successful adherence to these requirements, the TOE's conformance to the specified security functional requirements will have been demonstrated.
AVA_VAN.2	Refer to AGD_PRE.1 and AGE_OPE.1	A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities. The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Basic.