Hewlett-Packard Company Comware V7.1 Running on MSR2000, MSR3000, and MSR4000 Series Routers Security Target

Version 0.11
03/19/2015

Prepared for:

Hewlett-Packard Development Company, L.P.

11445 Compaq Center Drive West
Houston, Texas 77070

Prepared By:

Gossamer Laboratories
www.gossamersec.com

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Hewlett-Packard Comware V7.1 running on MSR2000, MSR3000, and MSR4000 Series Routers provided by Hewlett-Packard Development Company. Each Router is a stand-alone network appliance designed to implement a wide range of network layer 2 and 3 services, routing, and firewall capabilities.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- Extended Components Definition (Section 5)
- Security Requirements (Section 6)
- TOE Summary Specification (Section 7)

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 letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- The NDPP uses an additional convention – the 'case' – which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST and they are identified using **bold** text.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – Hewlett-Packard Company Comware V7.1 Running on MSR2000, MSR3000, and MSR4000 Series Routers Security Target

ST Version – Version 0.11

ST Date – 03/19/2015

1.2 TOE Reference

TOE Identification – Hewlett-Packard Company Comware V7.1.049 running on MSR2000, MSR3000, and MSR4000 Series Routers:

Product Series	Specific Devices
HP MSR2000 Series	MSR2003 AC Router (JG411A)
HP MSR3000 Series	MSR3012 AC Router (JG409A)
	MSR3024 AC Router (JG406A)
	MSR3044 Router (JG405A)
	MSR3064 Router (JG404A)
HP MSR4000 Series	MSR4060 Router Chassis (JG403A)
	MSR4080 Router Chassis (JG402A)

TOE Developer – Hewlett-Packard Company

Evaluation Sponsor – Hewlett-Packard Company

1.3 TOE Overview

The Target of Evaluation (TOE) is Hewlett-Packard Comware V7.1 running on MSR2000, MSR3000, and MSR4000 Series Routers. Each series of this router family consists of a set of distinct router devices (as identified in section 1.2) which vary primarily according to power delivery, performance, and port density. Each router in the MSR2000, MSR3000, and MSR4000 series is running the same Comware V7.1 software with only the modules applicable for the specific hardware installed. Each of the routers identified in section 1.2 satisfy all of the requirements defined by this evaluation. These routers are used to provide a network infrastructure supporting the routing of network traffic between connected networks.

While the routers have fixed ports, they also support plug-in modules, transceivers, memory, and power supplies that provide additional functionality (e.g., various numbers and types of network connection ports). These plug-in accessories do not serve to change the security characteristics of the TOE and as such can optionally be used in the evaluated configuration.

1.4 TOE Description

The HP routers are network routers which consist of hardware and software components. While the physical form factor of each distinct series in the router family is substantially different, the underlying hardware share a similar architecture. The software utilized is a common code base of a modular nature with only the modules applicable for the specific hardware installed.

MSR2000 Series Routers

The HP MSR2000 Router Series, the next generation of router from HP, is a component of the HP FlexBranch solution, which is a part of the comprehensive HP FlexNetwork architecture. These routers feature a modular design that delivers unmatched application services for small- to medium-sized branch offices. This gives your IT personnel the benefit of reduced complexity, and simplified configuration, deployment, and management.

The MSR2000 series provides a network infrastructure that enables you to quickly adapt to your changing business requirements while delivering integrated concurrent services on a single, easy-to-manage platform.

MSR3000 Series Routers

The HP MSR3000 Router Series, the next generation of router from HP, is a component of the HP FlexBranch solution, which is a part of the comprehensive HP FlexNetwork architecture. These routers feature a modular design that delivers unmatched application services for medium- to large-sized branch offices. This gives your IT personnel the benefit of reduced complexity, and simplified configuration, deployment, and management.

The MSR3000 routers use the latest multicore CPUs, offer Gigabit switching, provide an enhanced PCI bus, and ship with the latest version of HP Comware software to help ensure high performance with concurrent services. The MSR3000 series provides a full-featured routing platform with up to 5 Mpps forwarding capacity and 3.3 Gb/s of throughput. These routers also support HP Open Application Platform (OAP) modules to deliver integrated industry-leading HP AllianceOne partner applications such as virtualization, unified communications and collaboration (UC&C), and application optimization capabilities.

The MSR3000 series provides a network infrastructure that enables you to quickly adapt to changing business requirements while delivering integrated concurrent services on a single, easy-to-manage platform.

MSR4000 Series Routers

The HP MSR4000 Router Series, the next generation of router from HP, is a component of the HP FlexBranch solution, which is a part of the comprehensive HP FlexNetwork architecture. These routers feature a modular design that delivers unmatched application services for extra-large branch offices, headquarters, and campuses. This gives your IT personnel the benefit of reduced complexity, and simplified configuration, deployment, and management. The MSR4000 series leverages separated data and control planes, dual main processing units (MPUs), and support for up to four power supplies, which provides outstanding performance and reliability.

The MSR4000 routers provide a full-featured routing platform with the latest multicore CPUs, offer 10 Gigabit switching, provide an enhanced PCI bus, and ship with the latest version of HP Comware software to help ensure high performance with concurrent services. The MSR4000 series provides a full-featured routing platform with up to 20 Mpps forwarding capacity and 8 Gb/s of throughput. These routers also support HP Open Application Platform (OAP) modules to deliver integrated industry-leading HP AllianceOne partner applications such as virtualization, unified communications and collaboration (UC&C), and application optimization capabilities.

The MSR4000 series provides a network infrastructure that enables you to quickly adapt to your changing business requirements while delivering integrated concurrent services on a single, easy-to-manage platform.

1.4.1 TOE Architecture

The TOE is the Comware V7.1 software running in the context of a platform in the Hewlett-Packard MSR2000, MSR3000, and MSR4000 Series Routers. Section 1.2 identifies the specific models and revisions of router platform that are required for the TOE. Each router in the MSR2000, MSR3000, and MSR4000 series is running the same Comware V7.1 software with only the modules applicable for the specific hardware installed. The discussion below presents a high level hardware architecture followed by a description of the architecture of the Comware V7.1 software.

The hardware differences between the MSR2000, MRS3000 and MSR4000 series routers are summarized in section 1.4. The routers in these series all utilize the same multi-core processing design which is designed into various form-factors to support the different hardware interfaces to the router series. Figure 1 depicts the common multi-core processing unit that is part of all routers. This processing unit includes multiple CPUs and specialty processing capabilities for accelerating encryption and for processing of packet data.

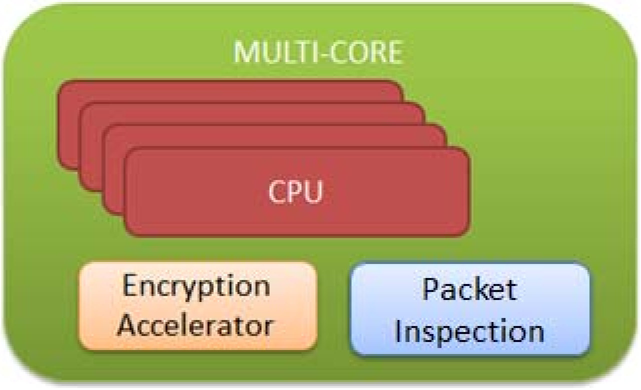

Figure 1 Multi-Core Processing Unit

The MSR2000 series routers are single Multi-Core Processing Unit routers, which provide SIC slots and Gigabit Ethernet (GbE) interfaces.

The MSR3000 series routers are single Multi-Core Processing Unit routers. The MSR3000 series routers also include a CUBE ASIC to provide the SIC slots, and enhanced PCI bus to provide the HMIM slots.

The MSR4000 includes a Main Processing Unit (MPU) and a Service Processing Unit (SPU) within its chassis. The MPU consists of Dual Multi-Core Processing Units. The SPU consists of a single Multi-Core Processing Unit with an enhanced PCI to provide the HMIM slots.

The remainder of this section focuses upon the software portion of the TOE.

The HP routers all share a common software code base – Comware V7.1. Comware is special purpose system software based on Linux that implements a wide array of networking technology, including: IPv4/IPv6 stacks, Ethernet switching, routing, etc.

Comware V7.1 comprises four planes: management plane, control plane, data plane, and infrastructure plane.

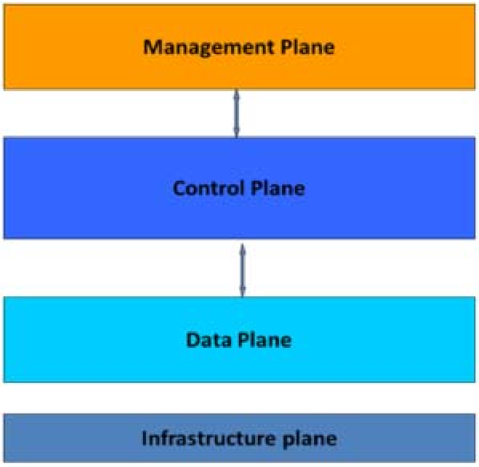

Figure 2 Comware V7.1 Planes

- ***Infrastructure plane* –** The 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* –** The data plane provides data forwarding for local packets and received IPv4 and IPv6 packets at different layers.

- ***Control plane* –** The 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* –** The management plane provides management interfaces for operators to configure, monitor, and manage Comware V7.1. Common management interfaces include SSHv2 and SNMPv3.

Comware V7.1 implements full modularization based on Linux. All software features run independent processes in different spaces. A failed process does not affect other processes. Preemptive scheduling used by Linux threads enables Comware V7.1 to provide high-speed services. In addition, Linux supports multi-core, multi-CPU, and Symmetrical Multi-Processing (SMP) technologies, which can maximize multi-CPU performance.

Comware V7.1 also supports Multitenant Device Contexts (MDC) where the data, control, and management planes are virtualized into multiple logical devices sharing the same kernel but having distinct data. Each MDC is assigned its own interfaces and CPU resources. This feature will be supported by the MSR routers in future releases of Comware 7.1.

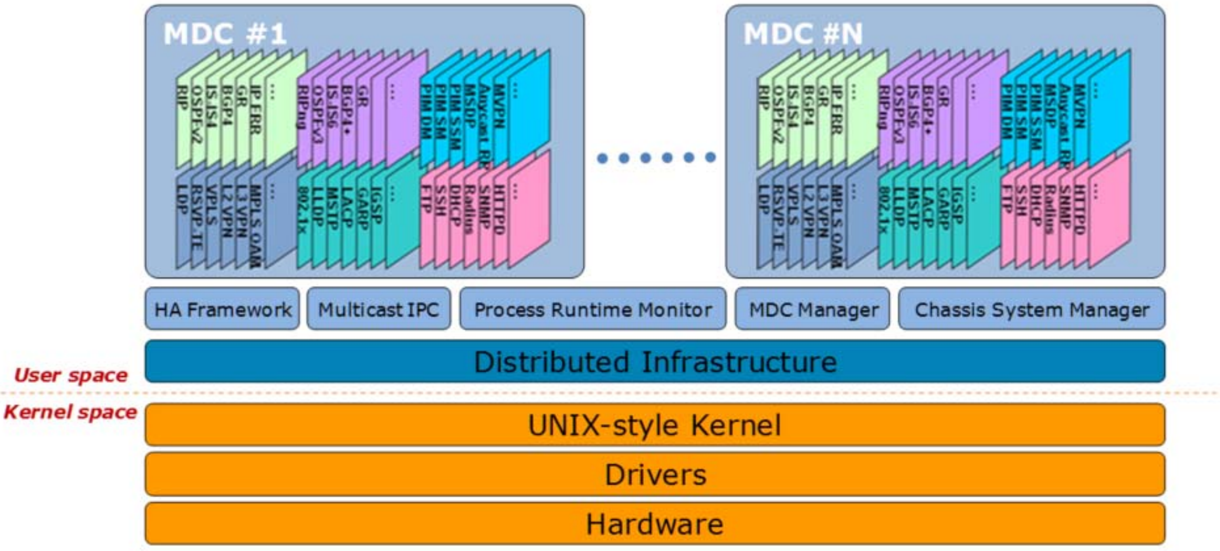

Figure 3 Comware V7.1 Modular Design

Underlying the main user space Comware components are the kernel and hardware-specific device drivers to provide necessary abstractions of the hardware components for the higher-level software components.

The user space Comware software components hosted in MDCs are composed of subsystems designed to implement applicable functions. For example there are subsystems dedicated to Management Information Base (MIB) and CLI management. There are also subsystems dedicated to the IPv4 and IPv6 network stacks as well as the applicable network protocols and forwarding, routing, etc.

From a security perspective, the TOE includes a cryptographic module that supports SSHv2 and SNMPv3. Otherwise, the TOE implements a wide range of network switching and routing protocols and functions.

More advanced firewall security features are also available (including packet filtering support).

The various TOE devices include the same security functions. The salient differences between the devices are the available ports and port adapters (supporting different pluggable modules), primarily representing differences in numbers, types, and speeds of available network connections.

1.4.1.1 Physical Boundaries

The hardware environment of the TOE is a physical network rack-mountable router that supports modules that serve to offer a wide range of network ports varying in number, form factor (copper or fiber), and performance (1 – 10 Gb). The TOE software executes entirely within the network router appliance.

Alternately, the hardware can be deployed as a pair of routers connected via a dedicated high-availability (HA) link so that the pair operates in a redundant manner allowing continued operations should one of the routers fail. In this scenario, both routers are running their own instance of the TOE – Comware V7.1 software.

The TOE can be configured to rely on and utilize a number of other components in its operational environment.

- SYSLOG server – to receive audit records when the TOE is configured to deliver them to an external log server.
- Radius and TACACS+ servers – The TOE can be configured to utilize external authentication servers.
- SNMP server – The TOE can be configured to issue and received SNMP traps. Note that the TOE supports SNMPv3.
- Management Workstation – The TOE supports CLI access and as such an administrator would need a terminal emulator (supporting SSHv2) to utilize those administrative interfaces.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by MSR Routers:

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

1.4.1.2.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and to send the logs to a designated external SYSLOG server to mitigate the possibility of losing audit records when available space becomes exhausted on the TOE.

Locally stored audit records can be reviewed and otherwise managed by an administrator.

1.4.1.2.2 Cryptographic support

The TOE includes a cryptographic module that provides key management and encryption/decryption features in support of higher level cryptographic protocols to provide a trusted path for remote administration.

1.4.1.2.3 User data protection

The TOE performs a wide variety of network switching and routing functions, passing network traffic among its various physical and logical (e.g., VLAN) network connections. While implementing applicable network protocols associated with network traffic forwarding, the TOE is carefully designed to ensure that it doesn’t inadvertently reuse data found in network traffic.

The TOE implements packet filtering that can be configured and monitored by an administrator.

1.4.1.2.4 Identification and authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console as well as network accessible interfaces (e.g., SSHv2) for interactive administrator sessions. A SNMPv3 interface, which also required proper user credentials, is available for non-interactive MIB based management of the TOE.

The TOE supports the local (i.e., on device) definition of users with usernames and roles that can be authenticated with passwords or certificates. The TOE supports roles to control permissions for administrators (i.e., Network Administrator and Security Auditor are administrator roles), these roles are defined in section 7.5. Additionally, the TOE can be configured to utilize the authentication services of trusted RADIUS and TACACS servers in the operational environment to support, for example, centralized user administration.

1.4.1.2.5 Security management

The TOE provides Command Line (CLI) commands and Management Interface Block (MIB) SNMPv3 interface to access the wide range of security management functions. Security management commands are limited to administrators only after they have provided acceptable user identification and authentication data to the TOE.

1.4.1.2.6 Protection of the TSF

The TOE provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

The TOE also performs self-tests when it starts up to ensure its cryptographic functions operate properly and that the Comware and TSF executable files are intact.

1.4.1.2.7 TOE access

The TOE can be configured to display advisory banners when users log in and will enforce an administrator-defined inactivity timeout value after which an inactive session will be terminated.

1.4.1.2.8 Trusted path/channels

The TOE protects communication with administrators using SSHv2 for CLI access. Access to the MIB interface is protected using SNMPv3. In each case, both integrity and disclosure protection is ensured.

The TOE protects communication with an associated SYSLOG server using IPsec primarily to protect exported audit records.

1.4.2 TOE Documentation

There are numerous documents that provide information and guidance for the deployment of Hewlett-Packard Routers. The following documents were specifically examined in the context of the evaluation:

- HP MSR2000/3000/4000 Router Series - MSR2000-MSR3000-MSR4000_R0007P12_Release-Notes-Portfolio
- HP MSR2000/3000/4000 Router Series Command References
- HP MSR2000/3000/4000 Router Series Security Command Reference
- HP MSR2000/3000/4000 Router Series ACL and QoS Command Reference
- HP MSR2000/3000/4000 Router Series MPLS Command Reference
- HP MSR2000/3000/4000 Router Series Layer 3 - IP Services Command Reference
- HP MSR2000/3000/4000 Router Series Layer 2 - WAN Command Reference
- HP MSR2000/3000/4000 Router Series Layer 3 - IP Routing Command Reference
- HP MSR2000/3000/4000 Router Series Fundamentals Command Reference
- HP MSR2000/3000/4000 Router Series Interface Command Reference

- HP MSR2000/3000/4000 Router Series Layer 2 - LAN Switching Command Reference
- HP MSR2000/3000/4000 Router Series Interface Module Guide
- HP MSR2000/3000/4000 Router Series Voice Command Reference
- HP MSR2000/3000/4000 Router Series High Availability Command Reference
- HP MSR2000/3000/4000 Router Series Network Management and Monitoring Command Reference
- HP MSR2000/3000/4000 Router Series Probe Command Reference
- HP MSR2000/3000/4000 Router Series IP Multicast Command Reference
- HP MSR2003 Router FIPS Enclosure Installation Guide
- HP MSR2000 Router Series Installation Guide
- HP MSR2000 Router Series Quick Start Guide
- HP MSR2000/3000/4000 Router Series Configuration Guides
- HP MSR2000/3000/4000 Router Series Fundamentals Configuration Guide
- HP MSR2000/3000/4000 Router Series Layer 3 - IP Services Configuration Guide
- HP MSR2000/3000/4000 Router Series Interface Configuration Guide
- HP MSR2000/3000/4000 Router Series Layer 3 - IP Routing Configuration Guide
- HP MSR2000/3000/4000 Router Series IP Multicast Configuration Guide
- HP MSR2000/3000/4000 Router Series MPLS Configuration Guide
- HP MSR2000/3000/4000 Router Series ACL and QoS Configuration Guide
- HP MSR2000/3000/4000 Router Series Security Configuration Guide
- HP MSR2000/3000/4000 Router Series Voice Configuration Guide
- HP MSR2000/3000/4000 Router Series Layer 2 - LAN Switching Configuration Guide
- HP MSR2000/3000/4000 Router Series Layer 2 - WAN Configuration Guide
- HP MSR2000/3000/4000 Router Series Network Management and Monitoring Configuration Guide
- HP MSR2000/3000/4000 Router Series High Availability Configuration Guide

Additional, on-line technical documentation and manuals can be found for the applicable TOE models and devices via the Resources link at the following URLs:

- HP MSR2000 Router Series overview

  http://h17007.www1.hp.com/us/en/networking/products/routers/HP_MSR2000_Router_Series/index.aspx
- HP MSR3000 Router Series overview

  http://h17007.www1.hp.com/us/en/networking/products/routers/HP_MSR3000_Router_Series/index.aspx
- HP MSR4000 Router Series overview

  http://h17007.www1.hp.com/us/en/networking/products/routers/HP_MSR4000_Router_Series/index.aspx

2. Conformance Claims

This TOE is 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
- Package Claims:
    - Assurance Level: EAL 3 augmented with ALC_FLR.2

2.1 Conformance Rationale

This ST is based on the Common Criteria and makes no conformance claims to a Protection Profile.

3. Security Problem Definition

The Security Problem Definition (composed of threat statements and assumption) is defined to reflect threats and assumption typical of a network device configured to serve as a firewall.

3.1 Threats

T.AUDACC Actions performed by users related to the security management of the TOE or by network entities using mediated routing functions of the TOE may not be known to the administrators due to actions not being recorded, records being lost, records not being accessible, or records being modified or deleted (by unauthorized users).

T.MEDIAT An unauthorized network entity may send impermissible information through the TOE which results in the exploitation of resources on an internal (protected) network.

T.NOAUTH An unauthorized user may attempt to impersonate an authorized user to access and use security functions and/or non-security functions provided by the TOE.

T.PROCOM An unauthorized user may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator or remote SYSLOG server and the TOE.

T.SELPRO An unauthorized user may read, modify, or destroy security critical TOE configuration data or authorized administrators may not have access to the functions necessary to manage the TOE security functions.

3.2 Assumptions

A.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.PHYSEC The TOE is physically secure.

A.PUBLIC The TOE does not host public data.

A.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

A.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.

4. Security Objectives

Like the Security Problem Definition, the Security Objectives have been designed to reflect the objectives for the TOE and its environment where the TOE is acting as a firewall for its environment.

4.1 Security Objectives for the TOE

O.ACCOUN The TOE must provide the ability to support user accountability for information flows through the TOE between network entities and for authorized administrator use of security functions.

O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

O.ENCRYP The TOE must protect the confidentiality of its dialogues with external SYSLOG servers and remote authorized administrators through encryption.

O.IDAUTH The TOE must be able to present an advisory banner of user responsibilities and identify and authenticate the claimed identity of all users before granting a user access to TOE functions and limit the potential for unattended session exposure after a user has been authenticated.

O.MEDIAT The TOE must be able to mediate the flow of information from network entities on a connected network to network entities on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions and must ensure that only authorized administrators are able to access such functionality.

4.2 Security Objectives for the Environment

OE.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.

OE.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

OE.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

OE.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

OE.PHYSEC The TOE is physically secure.

OE.PUBLIC The TOE does not host public data.

OE.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

OE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.

4.3 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

4.3.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

Note that while additional mappings (e.g., indirect or supporting) could be identified between the stated threats and objectives, the mapping below is intended to show the most direct correspondence.

	T.AUDACC	T.MEDIAT	T.NOAUTH	T.PROCOM	T.SELPRO	A.DIRECT	A.GENPUR	A.LOWEXP	A.NOEVIL	A.PHYSEC	A.PUBLIC	A.REMACC	A.SINGEN
O.ACCOUN	X												
O.AUDREC	X												
O.ENCRYP				X									
O.IDAUTH			X										
O.MEDIAT		X											
O.SECFUN					X								
OE.ADMTRA									X				
OE.DIRECT						X							
OE.GENPUR							X						
OE.LOWEXP								X					
OE.NOEVIL									X				
OE.PHYSEC										X			
OE.PUBLIC											X		
OE.REMACC												X	
OE.SINGEN													X

Table 4-1 Environment to Objective Correspondence

4.3.1.1 T.AUDACC

Actions performed by users related to the security management of the TOE or by network entities using mediated routing functions of the TOE may not be known to the administrators due to actions not being recorded, records being lost, records not being accessible, or records being modified or deleted (by unauthorized users).

This Threat is satisfied by ensuring that:

- O.ACCOUN: This security objective is necessary to counter the threat: T.AUDACC because it requires that users can be held accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions.
- O.AUDREC: This security objective is necessary to counter the threat: T.AUDACC by requiring a readable and reliable audit trail and a means to search and sort the information contained in the audit trail.

4.3.1.2 T.MEDIAT

An unauthorized network entity may send impermissible information through the TOE which results in the exploitation of resources on an internal (protected) network.

This Threat is satisfied by ensuring that:

- O.MEDIAT: This security objective is necessary to counter the threat: T. which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

4.3.1.3 T.NOAUTH

An unauthorized user may attempt to impersonate an authorized user to access and use security functions and/or non-security functions provided by the TOE.

This Threat is satisfied by ensuring that:

- O.IDAUTH: This security objective is necessary to counter the threat: T.NOAUTH because it requires that users can be provided advisory notices, users must be identified and authenticated before accessing the TOE, and the risk of unattended sessions exposure is limited.

4.3.1.4 T.PROCOM

An unauthorized user may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator or remote SYSLOG server and the TOE.

This Threat is satisfied by ensuring that:

- O.ENCRYP: This security objective is necessary to counter the threat: T.PROCOM by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely and also be requiring that external SYSLOG communications are protected using encryption.

4.3.1.5 T.SELPRO

An unauthorized user may read, modify, or destroy security critical TOE configuration data or authorized administrators may not have access to the functions necessary to manage the TOE security functions.

This Threat is satisfied by ensuring that:

- O.SECFUN: The security objective is necessary to counter the threat: T.SELPRO by requiring that functions necessary to manage the TOE security functions are available to authorized administrators and only to authorized administrators.

4.3.1.6 A.DIRECT

Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

This Assumption is satisfied by ensuring that:

- OE.DIRECT: Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

4.3.1.7 A.GENPUR

There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

This Assumption is satisfied by ensuring that:

- OE.GENPUR: There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

4.3.1.8 A.LOWEXP

The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

This Assumption is satisfied by ensuring that:

- OE.LOWEXP: The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

4.3.1.9 A.NOEVIL

Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

This Assumption is satisfied by ensuring that:

- OE.NOEVIL: Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- OE.ADMTRA: Authorized administrators will receive the proper training.

4.3.1.10 A.NOREMO

Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.

This Assumption is satisfied by ensuring that:

- OE.NOREMO: Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.

4.3.1.11 A.PHYSEC

The TOE is physically secure.

This Assumption is satisfied by ensuring that:

- OE.PHYSEC: The TOE is physically secure.

4.3.1.12 A.PUBLIC

The TOE does not host public data.

This Assumption is satisfied by ensuring that:

- OE.PUBLIC: The TOE does not host public data.

4.3.1.13 A.REMACC

Authorized administrators may access the TOE remotely from the internal and external networks.

This Assumption is satisfied by ensuring that:

- OE.REMACC: Authorized administrators may access the TOE remotely from the internal and external networks.

4.3.1.14 A.SINGEN

Information cannot flow among the internal and external networks unless it passes through the TOE.

This Assumption is satisfied by ensuring that:

- OE.SINGEN: Information cannot flow among the internal and external networks unless it passes through the TOE.

5. Extended Components Definition

There are no extended requirements in this Security Target.

6. Security Requirements

The security requirements in this section have been drawn from the Common Criteria and are defined to address the security objectives defined in this Security Target.

6.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Hewlett-Packard MSR2000, MSR3000, and MSR4000 Series Routers Running Comware V7.1TOE.

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.1a: Cryptographic key generation (AES)
	FCS_CKM.1b: Cryptographic key generation (RSA)
	FCS_CKM.4: Cryptographic key destruction
	FCS_COP.1a: Cryptographic operation (AES)
	FCS_COP.1b: Cryptographic operation (Keyed Hash)
	FCS_COP.1c: Cryptographic operation (RSA)
FDP: User data protection	FDP_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	FIA_SOS.1: Verification of secrets
	FIA_UAU.1: Timing of authentication
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
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_TAB.1: Default TOE access banners
FTP: Trusted path/channels	FTP_TRP.1: Trusted path
	FTP_ITC.1: Inter-TSF trusted channel

Table 6-1 TOE Security Functional Components

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.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 relevant auditable events for the [***not specified***] level of audit; and

c) [**the events in Table 6-2**].

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; 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 6-2**].

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_SAR.1	None.	
FAU_SAR.3	None.	
FAU_STG.1	None.	
FAU_STG.4	None.	
FCS_CKM.1a	None.	
FCS_CKM.1b	None.	
FCS_CKM.4	None.	
FCS_COP.1a	None.	
FCS_COP.1b	None.	
FCS_COP.1c	None.	
FDP_IFC.1	None.	
FDP_IFF.1	Decisions to permit requested information flows.	The presumed addresses of the source and destination subject.
FDP_RIP.2	None.	
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_ATD.1	None.	
FIA_SOS.1	Rejection by the TSF of any tested secret.	No additional information.
FIA_UAU.1	Any use of the authentication mechanism.	The user identities provided to the TOE.
FIA_UAU.5	The final decision on authentication.	The user identities provided to the TOE.
FIA_UID.2	All use of the user identification Mechanism.	The user identities provided to the TOE.
FMT_MOF.1	Covered by FMT_SMF.1	
FMT_MSA.1	Covered by FMT_SMF.1	
FMT_MSA.3	Covered by FMT_SMF.1	
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 per FMT_SMR.1.	The identity of the administrator performing the modification and the user identity being associated with the

Requirement	Auditable Events	Additional Audit Record Contents
		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.
FPT_TST.1	None.	
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	No additional information.
FTA_TAB.1	None.	
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 6-2 Auditable Events

6.1.1.2 User identity association (FAU_GEN.2)

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.

6.1.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1

The TSF shall provide [**a Security Auditor**] 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.

6.1.1.4 Selectable audit review (FAU_SAR.3)

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].

6.1.1.5 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1

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

FAU_STG.1.2

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

6.1.1.6 Prevention of audit data loss (FAU_STG.4)

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.

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation (FCS_CKM.1a) (AES)

FCS_CKM.1a.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**AES key generation**] and specified cryptographic key sizes [**128, 192 and 256-bits**] that meet the following: [**FIPS 197**].

6.1.2.2 Cryptographic key generation (FCS_CKM.1b) (RSA)

FCS_CKM.1b.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 PUB 186-3**].

6.1.2.3 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1

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

6.1.2.4 Cryptographic operation (FCS_COP.1a) (AES)

FCS_COP.1a.1

The TSF shall perform [**AES encryption and decryption in support of SSHv2, SNMPv3 and IPsec**] in accordance with a specified cryptographic algorithm [**AES operating in CBC mode**] and cryptographic key sizes [**128, 192 or 256-bits**] that meet the following: [**FIPS PUB 197, "Advanced Encryption Standard (AES)"**].

6.1.2.5 Cryptographic operation (FCS_COP.1b) (Keyed Hash)

FCS_COP.1b.1

The TSF shall perform [**keyed-hash message authentication in support of SSHv2, SNMPv3 and IPsec**] in accordance with a specified cryptographic algorithm [**HMAC-SHA-1 or HMAC-SHA-1-96**] and cryptographic key sizes **[160 bits]** that meet the following: [**FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-4, "Secure Hash Standard"**].

6.1.2.6 Cryptographic operation (FCS_COP.1c) (RSA)

FCS_COP.1c.1

The TSF shall perform [**RSA cryptographic signature services (verification) in support of SSHv2 and IPsec authentication**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**2048 bits**] that meet the following: [**FIPS PUB 186-3, "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes**]

6.1.3 User data protection (FDP)

6.1.3.1 Subset information flow control (FDP_IFC.1)

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].

6.1.3.2 Simple security attributes (FDP_IFF.1)

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.**]

6.1.3.3 Full Residual Information Protection (FDP_RIP.2)

FDP_RIP.2.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] all objects.

6.1.4 Identification and authentication (FIA)

6.1.4.1 Authentication failure handling (FIA_AFL.1)

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**].

6.1.4.2 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1

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

a) identity;

b) association of a human user with an administrative role].

6.1.4.3 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1

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

a) each locally defined user password must be a minimum of 15 characters in length;

b) 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].

6.1.4.4 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1

The TSF shall allow [**identification as stated in FIA_UID.2**] behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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

6.1.4.5 Multiple authentication mechanisms (FIA_UAU.5)

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:**

a) **SNMP authentication is performed by the TOE and can be configured on a per-user basis to require authentication using a password,**
b) **SSH authentication can be configured on the TOE on a per-user basis to require a password, or both a password and RSA certificate;**
c) **SSH and console authentication utilize only those authentication mechanisms configured by a Network Administrator;**
d) **SSH and console authentication check the configured authentication mechanisms in the order they are configured by a Network Administrator**].

6.1.4.6 User identification before any action (FIA_UID.2)

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.

6.1.5 Security management (FMT)

6.1.5.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1

The TSF shall restrict the ability to perform[1] the functions: [**the functions shown in Table 6-3**] to [**the roles as shown in Table 6-3**].

Role	Function
Network Administrator	a) start-up and re-boot the TOE; b) create, delete, modify, and view information flow security policy rules that permit or deny information flows; c) create, delete, modify, and view user attributes that identify authorized users and their associated role; d) modify and set the locking period and threshold for the number of permitted authentication attempt failures; e) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures; f) modify and set the time and date; and g) enable, disable, and configure external RADIUS and TACACS+ services
Security Auditor	a) archive, create, delete, empty, and review the audit trail

Table 6-3 Role to Admin Function Mapping

6.1.5.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1

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

6.1.5.3 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1

The TSF shall enforce the [**UNAUTHENTICATED SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

[1] While the selection in the CC allows functions such as modify, determine, enable, and disable, the SFR has been refine to simply indicate ‘perform’ and specific actions are associated with each function in the subsequent list.

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.

6.1.5.4 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [**the functions identified in FMT_MOF.1, FMT_MSA.1 and FMT_MSA.3**].

6.1.5.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1

The TSF shall maintain the roles [**Network Administrator and Security Auditor**].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

6.1.6.2 TSF testing (FPT_TST.1)

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]***].

6.1.7 TOE access (FTA)

6.1.7.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1

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

6.1.7.2 Default TOE access banners (FTA_TAB.1)

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

6.1.8 Trusted path/channels (FTP)

6.1.8.1 Inter-TSF trusted channel (FTP_ITC.1)

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 **using encryption**.

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 serve**r].

6.1.8.2 Trusted path (FTP_TRP.1)

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 [***modification, disclosure***] **using encryption**.

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]***].

6.2 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.ACCOUN	O.AUDREC	O.ENCRYP	O.IDAUTH	O.MEDIAT	O.SECFUN
FAU_GEN.1	X	X				
FAU_GEN.2	X					
FAU_SAR.1		X				
FAU_SAR.3		X				
FAU_STG.1						X
FAU_STG.4	X					
FCS_CKM.1a			X			
FCS_CKM.1b			X			
FCS_CKM.4			X			
FCS_COP.1a			X			
FCS_COP.1b			X			
FCS_COP.1c			X			
FDP_IFC.1					X	
FDP_IFF.1					X	
FDP_RIP.2					X	
FIA_AFL.1				X		
FIA_ATD.1				X		
FIA_SOS.1				X		

	O.ACCOUN	O.AUDREC	O.ENCRYP	O.IDAUTH	O.MEDIAT	O.SECFUN
FIA_UAU.1				X		
FIA_UAU.5				X		
FIA_UID.2	X			X		
FMT_MOF.1						X
FMT_MSA.1					X	
FMT_MSA.3					X	X
FMT_SMF.1						X
FMT_SMR.1						X
FPT_STM.1		X				
FPT_TST.1			X			X
FTA_SSL.3				X		
FTA_TAB.1				X		
FTP_ITC.1			X			
FTP_TRP.1			X			

Table 6-4 Objective to Requirement Correspondence

6.2.1 O.ACCOUN

The TOE must provide the ability to support user accountability for information flows through the TOE between network entities and for authorized administrator use of security functions.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: This component outlines what data must be included in audit records and what events must be auditable. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
- FAU_GEN.2: This component requires that audit records be traceable to users. This component traces back to and aids in meeting the following objective: O.ACCOUN.
- FAU_STG.4: This component helps to ensure accountability by requiring that the TOE can export audit records to an external audit server so they are not lost when the TOE overwrites its audit records when it runs out of available storage space.
- FIA_UID.2: This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

6.2.2 O.AUDREC

The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: This component outlines what data must be included in audit records and what events must be auditable. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
- FAU_SAR.1: This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

- FAU_SAR.3: This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.
- FPT_STM.1: FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

6.2.3 O.ENCRYP

The TOE must protect the confidentiality of its dialogues with external SYSLOG servers and remote authorized administrators through encryption.

This TOE Security Objective is satisfied by ensuring that:

- FCS_CKM.1a: This component ensures that keys can be generated in support of FCS_COP.1a. This component traces back to and aids in meeting the following objective: O.ENCRYP.
- FCS_CKM.1b: This component ensures that keys can be generated in support of FCS_COP.1d. This component traces back to and aids in meeting the following objective: O.ENCRYP.
- CS_CKM.4: This component ensures that keys related to FCS_COP.1a are appropriately destroyed. This component traces back to and aids in meeting the following objective: O.ENCRYP.
- FCS_COP.1a: This component ensures that if the TOE does support an administrator's ability to communicate with the TOE remotely from an internal or external network that AES is used to encrypt and decrypt such traffic. This component also ensures that AES is used to encrypt and decrypt IPsec traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP.
- FCS_COP.1b: This component ensures that the TOE utilizes HMAC-SHA-1 and HMAC-SHA-1-96 when performing keyed hashing message authentication for SSHv2, SNMPv3 and IPsec. This component traces back to and aids in meeting the following objective: O.ENCRYP.
- FCS_COP.1c: This component ensures that the TOE utilizes RSA when performing cryptographic verification services for SSHv2 and IPsec. This component traces back to and aids in meeting the following objective: O.ENCRYP.FPT_TST.1: This component ensures that the cryptographic functions are tested during TOE start-up to ensure they are working correctly. This component traces back to and aids in meeting the following objectives: O.ENCRYP and O.SECFUN.
- FTP_ITC.1: This component ensures that connections to external SYSLOG servers are secured using encryption. This component traces back to and aids in meeting the following objective: O.ENCRYP.
- FTP_TRP.1: This component ensures that administrators communicating with the TOE remotely from an internal or external network have access to a trusted path protected using encryption. This component traces back to and aids in meeting the following objective: O.ENCRYP.

6.2.4 O.IDAUTH

The TOE must be able to present an advisory banner of user responsibilities and identify and authenticate the claimed identity of all users before granting a user access to TOE functions and limit the potential for unattended session exposure after a user has been authenticated.

This TOE Security Objective is satisfied by ensuring that:

- FIA_AFL.1: This component ensures that human users who are not authorized cannot endlessly attempt to authenticate. After some number of failures the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator re-enables that user. This component traces back to and aids in meeting the following objective: O.IDAUTH.
- FIA_ATD.1: This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role(s) chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objective: O.IDAUTH.
- FIA_SOS.1: This component ensures that non-trivial passwords are used to help ensure that unauthorized users cannot readily guess the password of an authorized user to assume their identity. This component traces back to and aids in meeting the following objective: O.IDAUTH.

- FIA_UAU.1: This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. This component traces back to and aids in meeting the following objective: O.IDAUTH.
- FIA_UAU.5: This component works in conjunction with FIA_UAU.1 allowing alternate authentication mechanisms to be employed by the TOE. This component traces back to and aids in meeting the following objective: O.IDAUTH.
- FIA_UID.2: This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.
- FTA_SSL.3: This component was chosen to help mitigate that possibility of inappropriate access (without being identified and authenticated) obtained by using a session that was not locked or logged off properly by ensuring that the TSF would terminate inactive sessions. This component traces back to and aids in meeting the following objective: O.IDAUTH.
- FTA_TAB.1: This component was chosen to require that users can be made aware of their responsibilities prior to logging into the TOE to perform security functions. This component traces back to and aids in meeting the following objective: O.IDAUTH.

6.2.5 O.MEDIAT

The TOE must be able to mediate the flow of information from network entities on a connected network to network entities on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.1: This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.
- FDP_IFF.1: This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.
- FDP_RIP.2: This component ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.
- FMT_MSA.1: This component ensures that the information flow control security rules can be managed only by an administrator. This component traces back to and aids in meeting the following objective: O.MEDIAT.
- FMT_MSA.3: This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECFUN.

6.2.6 O.SECFUN

The TOE must provide functionality that enables an authorized administrator to use the TOE security functions and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.1: This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objective: O.SECFUN.

- FMT_MOF.1: This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objective: O.SECFUN.
- FMT_MSA.3: This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECFUN.
- FMT_SMF.1: This component ensures that suitable security management functions are available to the administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.
- FMT_SMR.1: Each of the CC class FMT components in this Protection Profile depend on this component. It requires the PP/ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.
- FPT_TST.1: The TOE provides the capability to verify the integrity of Comware executable file and the rest of the TSF executable code to help ensure that the TOE security functions will work properly to ensure protected access to the TOE security management functions. This component traces back to and aids in meeting the following objectives: O.ENCRYPT and O.SECFUN.

6.3 TOE Security Assurance Requirements

The SARs for the TOE are the EAL 3 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: Authorization 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
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 6-5 EAL 3 augmented with ALC_FLR.2 Assurance Components

6.3.1 Development (ADV)

6.3.1.1 Security architecture description (ADV_ARC.1)

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 initialization 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.

6.3.1.2 Functional specification with complete summary (ADV_FSP.3)

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 security enforcing effects and exceptions associated with invocation of the TSFI.

ADV_FSP.3.6c

The functional specification shall summarize 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.

6.3.1.3 Architectural design (ADV_TDS.2)

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 summarize the SFR-supporting and SFR-non-interfering behavior of the SFR-enforcing subsystems.

ADV_TDS.2.6c

The design shall summarize the behavior of the SFR-supporting subsystems.

ADV_TDS.2.7c

The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.2.8c

The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

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.

6.3.2 Guidance documents (AGD)

6.3.2.1 Operational user guidance (AGD_OPE.1)

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.

6.3.2.2 Preparative procedures (AGD_PRE.1)

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.

6.3.3 Life-cycle support (ALC)

6.3.3.1 Authorization controls (ALC_CMC.3)

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.3.1c

The TOE shall be labeled 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 authorized 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.

6.3.3.2 Implementation representation CM coverage (ALC_CMS.3)

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; 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.

6.3.3.3 Delivery procedures (ALC_DEL.1)

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.

6.3.3.4 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d

The developer shall produce 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.

6.3.3.5 Flaw reporting procedures (ALC_FLR.2)

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 user's 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.

6.3.3.6 Developer defined life-cycle model (ALC_LCD.1)

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.

6.3.4 Tests (ATE)

6.3.4.1 Analysis of coverage (ATE_COV.2)

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.

6.3.4.2 Testing: basic design (ATE_DPT.1)

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.

6.3.4.3 Functional testing (ATE_FUN.1)

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.

6.3.4.4 Independent testing - sample (ATE_IND.2)

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.

6.3.5 Vulnerability assessment (AVA)

6.3.5.1 Vulnerability analysis (AVA_VAN.2)

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.

6.4 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs), which correspond to EAL3 augmented with ALF_FLR.2, in this ST have been adopted to represent a reasonable level of security assurance commensurate with that needed for a network router.

6.5 Requirement Dependency Rationale

As can be seen in the following table all of the SFR and SAR dependencies are satisfied in this ST.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UID.2
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_GEN.1	FAU_GEN.1
FCS_CKM.1a	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	FCS_COP.1a and FCS_CKM.4

ST Requirement	CC Dependencies	ST Dependencies
FCS_CKM.1b	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	FCS_COP.1b and FCS_CKM.4
FCS_CKM.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1 (all iterations)
FCS_COP.1a	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1a and FCS_CKM.4
FCS_COP.1b	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1a and FCS_CKM.4
FCS_COP.1d	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1b and FCS_CKM.4
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1 and FMT_MSA.3
FDP_RIP.2	none	none
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	none	none
FIA_SOS.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UAU.5	none	none
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_IFC.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_STM.1	none	none
FPT_TST.1	none	none
FTA_SSL.3	FIA_UAU.1	FIA_UAU.1
FTA_TAB.1	none	none
FTP_ITC.1	none	none
FTP_TRP.1	none	none
ADV_ARC.1	ADV_FSP.1 and ADV_TDS.1	ADV_FSP.3 and ADV_TDS.2
ADV_FSP.3	ADV_TDS.1	ADV_TDS.2
ADV_TDS.2	ADV_FSP.3	ADV_FSP.3
AGD_OPE.1	ADV_FSP.1	ADV_FSP.3
AGD_PRE.1	None	None
ALC_CMC.3	ALC_CMS.1, ALC_DVS.1 and ALC_LCD.1	ALC_CMS.3, ALC_DVS.1, and ALC_LCD.1
ALC_CMS.3	None	None
ALC_DEL.1	None	None
ALC_DVS.1	None	None
ALC_FLR.2	None	None
ALC_LCD.1	None	None
ATE_COV.2	ADV_FSP.2 and ATE_FUN.1	ADV_FSP.3 and ATE_FUN.1
ATE_DPT.1	ADV_ARC.1, ADV_TDS.2, and ATE_FUN.1	ADV_ARC.1, ADV_TDS.2 and ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.2
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1 and ATE_FUN.1	ADV_FSP.3, AGD_OPE.1, AGD_PRE.1, ATE_COV.2 and ATE_FUN.1
AVA_VAN.2	ADV_ARC.1, ADV_FSP.2,	ADV_ARC.1, ADV_FSP.3,

ST Requirement	CC Dependencies	ST Dependencies
	ADV_TDS.1, AGD_OPE.1 and AGD_PRE.1	ADV_TDS.2, AGD_OPE.1 and AGD_PRE.1

Table 6-6 Requirement Dependencies

7. TOE Summary Specification

This chapter describes the security functions:

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

7.1 Security audit

The TOE is designed to be able to generate log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function as well as all of the events identified in Table 6-2 Auditable Events.

In general, the logged audit records identify the date and time, 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 (e.g., user) responsible for the event (e.g., user or network host). The logged audit records also include event-specific content that includes at least all of the content required in Table 6-2 Auditable Events.

The TOE includes an internal log implementation that can be used to store and review audit records locally. This internal log is maintained in a local file called ‘seclog.log’ file. This file contains every security relevant event generated by the TOE. The internal audit log operates as a circular buffer that overwrites the oldest records when it becomes full. The TOE can be configured to send generated audit records to an external SYSLOG server in to mitigate the possibility of losing audit records.

The internal log (seclog.log) can be accessed only by a user in the Security Auditor role, who can review, delete (but not modify), or archive stored audit records using available CLI commands specifically designed for the management of the internal LOG. The functions available to review audit records allow the audit records to be sorted in forward or reverse order according to date/time and to be searched using regular expressions.

NOTE: The TOE also maintains another set of log files “log-buffer” and “logfile#.log” which contains every log message generated by the TOE (security relevant and non-security relevant). These logs are in addition to and distinct from the internal log (seclog.log) described above.

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

- FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function and all other events identified in Table 6-2 Auditable Events. 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 6-2 Auditable Events.
- 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 internal log (seclog.log) can be fully reviewed by a user in the Security Auditor 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: Audit records in the internal log (seclog.log) can be deleted only by a user in the Security Auditor role and are not otherwise subject to modification.
- FAU_STG.4: The TOE overwrites the oldest audit records in the internal audit log (seclog.log) with new audit records when it becomes full. The TOE can be configured to send audit records to an external SYSLOG server as they are recorded.

7.2 Cryptographic support

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

The TOE uses a random number generator to generate keys of 128, 192 or 256-bits to support AES CBC encryption. 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 180-4. The TOE generates RSA key pairs of 2048 bits in accordance with FIPS PUB 186-3, “Digital Signature Standard (DSS)”, Appendix B.3 for RSA schemes.

The TOE supports SNMPv3 using AES (CBC) with 128 bit keys in conjunction with HMAC-SHA-1-96. The TOE implementation of SHA-1 meets FIPS PUB 180-4.

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 is designed to satisfy the following security functional requirements:

- FCS_CKM.1a: The TOE uses a random number generator to generate keys to support its AES key generation implementation.
- FCS_CKM.1b: The TOE uses a random number generator to generate keys to support its RSA key generation implementation.
- FCS_CKM.4: The TOE zeroizes cryptographic keys when they are no longer needed.
- FCS_COP.1a: The TOE implements AES using CBC mode to support its secure IPsec, SNMPv3 and SSHv2 protocols.
- FCS_COP.1b: The TOE implements HMAC-SHA-1 and HMAC-SHA-1-96 for use with SSHv2, SNMPv3 and IPsec.
- FCS_COP.1d: The TOE implements RSA to perform the encryption and decryption operations necessary to verify RSA certificates associated with SSH and IPsec authentication.

7.3 User data protection

The TOE is designed to ensure its own internal integrity as well as to protect user data from potential, unintended reuse by clearing resources (e.g., memory) as they are allocated to create objects used in the implementation of the TOE operations. Note that volatile memory is the primary resource involved in normal TOE execution while its persistent storage is based on non-volatile flash memory.

The TOE includes firewall functions that allow the definition of firewall rules, collectively known as access control lists (ACLs), that are applied to applicable network traffic as it is received and 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, other header fields (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 the Network Administrator to be either as configured (i.e., rules are processed in the order they are defined by the Network Administrator) 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 will be denied by default.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE implements an unauthenticated 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 (ack, fin, psh, rst, syn, urg)..
- FDP_RIP.2: The TOE always overwrites resources when allocated for use in objects.

7.4 Identification and authentication

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

In the evaluated configuration, users can connect to the TOE via a local console or remotely using SNMPv3 or SSHv2. In each case, the user is required to log in prior to successfully establishing a session through which TOE functions can be exercised.

When connecting to the TOE using SNMPv3 an administrator utilizes the TOE implementation of the SNMPv3 user-based security model (USM). As such, the user name provided must be defined within the TOE’s set of defined SNMPv3 users and the user must provide their password. That is, a remote user must provide a user name and password in order to use the SNMPv3 MIB interface. The user community permitted to access the TOE through SNMPv3 is independent from the locally defined user community which can utilize console and SSH logins. Each SNMPv3 user is an authorized administrator and has permission to issue MIBs based upon the SNMPv3 group assigned to the username.

In order to log in at a console or through SSH, the user must provide an identity and also authentication data (e.g., password or password with RSA credentials used in conjunction with an SSH session) that matches the provided identity. 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]

[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.

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(s) 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.

By default only local authentication will be used, but a Network Administrator 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) (see section 7.5) 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 reentering their identity and authentication data, in order to regain access to their locked session.

If a user fails to log in a Network Administrator 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 Administrator administrator).
- 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 role of Security Auditor 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.

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

- FIA_AFL.1: The administrator in a Network Administrator 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 the administrator in a Network Administrator 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). Locally defined SNMPv3 users are assigned identities, passwords and SNMPv3 group[4].

- 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.1: Prior to being authentication the TOE only allows users to identify themselves.

- 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_UID.2: The TOE doesn't offer any services or access to its functions without requiring a user to be identified.

[3] Local authentication for SSH can be password-based, certificate-based or both.
[4] The SNMPv3 group defines the administrative role for that user identity.

7.5 Security management

The TOE implements a role mechanism that is used to specify the role(s) and corresponding permissions which authenticated users possess. Table 7-1 defines the predefined roles and corresponding permissions that are implemented by the TOE.

Users with the network-admin or level-15 roles 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 roles can perform only some of the management functions assigned to the Network Administrator role (e.g., network operators can perform display operations not associated with auditing). Users with Level-2 through level-8 and level-10 through level-14 have no default permissions.

The Security Auditor role from FMT_SMR.1 corresponds to users in the role of security-audit. A user with the security-audit role cannot have any other role.

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) NOTE: On the routers in the MSR3000 Series and MSR4000 Series, the network-admin role has the same access to security auditing features as the security-audit role.
Security-audit	Security log manager. The user role 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 user 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 privilege-level-1)
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. If you are logged in with a local user account that has a level-9 user role, you can change the password in the local user account. Level-9 access rights are configurable. o RBAC non-debugging commands. o Local users. o File management. o Device management.

	o The display history-command all command. level-15—Has the same rights as network-admin.

Table 7-1 Role Definitions

Use of the level-0 through level-14 roles, as well as, the network-operator role is not required in order to properly administer a 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 Administrator. 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 TOE includes a SNMPv3 MIB interface that can alternately be used to manage some security configuration settings. Users able to use the SNMPv3 interface are constrained to operations permitted by the SNMPv3 group to which the SNMPv3 user is assigned, not by the TOE's role mechanism.

The TOE offers command-line interface providing a range of security management functions for use by a Network Administrator or Security Auditor. Among the functions available to the Network Administrator are those functions that are necessary to manage all aspects of the cryptographic functions of the TOE, those necessary to enable or disable the network services offered by the TOE, and the functions necessary to review the TOE versions, update the TOE components, and also to verify the validity of those updates.

The TOE also offers the following functions, which are limited to the Network Administrator:

- Start-up and re-boot the TOE,
- Manage the firewall rules (create, delete, modify, and view information flow security policy rules that permit or deny information flows),
- Manage user account definitions (create, delete, modify, and view user attributes that identify authorized users and their associated role(s)),
- Manage password failure constraints (modify and set the threshold for the number of permitted authentication attempt failures),
- Restoration of disabled users (restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures),
- Manage the internal clock (modify and set the time and date), and
- Manage remote authentication capabilities (enable, disable, and configure external RADIUS and TACACS+ services).

The TOE offers the following functions, limited to the Security Auditor:

- Manage the internal audit log (archive, create, delete, empty, and review the audit trail).

The MIB interface offered by the TOE can be used to perform a subset of the operations available using the command line interface. A network-admin must explicitly define the MIBs which each SNMPv3 group is permitted to perform, and assign each SNMPv3 user with a SNMPv3 group appropriate for that user.

The TOE imposes a restrictive default behavior in regard to its firewall policy by virtue of the fact that if there are no matching rules, the traffic is dropped. This default behavior can in effective be modified by a Network Administrator by defining one or more firewall rules that would serve to match all network traffic that might be received by the TOE.

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

- FMT_MOF.1: The TOE restricts the access to manage the TOE security functions to Network Administrator or Security Auditor.

- FMT_MSA.1: The TOE restricts access to modify the information flow rules to Network Administrator or Security Auditor.

- FMT_MSA.3: The TOE implements a restrictive default firewall policy by dropping network traffic when there are no matching rules. Only a Network Administrator can change that default by defining rules that are capable of matching and taking specifically configured actions for all network traffic the TOE might receive.

- FMT_SMF.1: The TOE includes the functions necessary manage the TOE corresponding to the restrictions defined in FMT_MOF.1.
- FMT_SMR.1: A Network Administrator corresponds to users in the TOE predefined role of network-admin or level-15. A Security Auditor corresponds to users in the TOE predefined role of security-audit.

7.6 Protection of the TSF

The hardware of the TOE is a router that includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes clock-related functions for use by the TOE. The TOE software can also be configured to utilize the NTP protocol to keep the local hardware-based real-time clock synchronized with other network devices.

During start-up of the TOE, the TOE first checks the integrity of the Comware and TSF executable files, and then runs a series of self-tests to ensure it is performing its cryptographic functions correctly. If any of these checks fails, the device will halt and require Network Administrator intervention to successfully start-up.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_STM.1: The TOE includes its own hardware clock.
- FPT_TST.1: The TOE includes the ability to test its cryptographic functions and the Comware and TSF executable files during start-up.

7.7 TOE access

The TOE can be configured by an administrator (in the Network Administrator 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 session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated.

The user will be required to re-enter their user id and their password so they can be re-authenticated in order to establish a new session.

The TOE can be configured to display administrator-configured advisory banners that will be displayed in conjunction with user login prompts. The banner contents are configured by a user in the Network Administrator role.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE terminates interactive sessions that have been inactive for an administrator-configured period of time. This period is configured by a user in the Network Administrator role.
- FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners when users establish interactive sessions with the TOE. The banner contents are configured by a user in the Network Administrator role.

7.8 Trusted path/channels

To support secure remote administration, the TOE includes implementations of SSHv2 and SNMPv3. In each case, a remote host (presumably acting on behalf of an administrator) can initiate a secure remote connection for the purpose of security management. Note that only the local console is available by default and each of these remote administration services can be independently enabled by a Network Administrator.

In the case of SNMPv3, the TOE acts as a SNMPv3 server accepting non-interactive Management Information Base (MIB) options from an authenticated source. SNMPv3 requires the client to be authenticated against a locally configured user base and utilizes AES-128 in order to protect this security management channel.

In the case of SSHv2, the TOE offers secure command line interface (CLI) interactive administrator sessions. An administrator with appropriate SSHv2 capable clients can establish secure remote connections with the TOE. However, to successfully establish such an interactive session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to issue commands within their assigned authorizations.

As indicated earlier, the TOE can be configured to export audit records to an external SYSLOG server. In order to protect exported audit records from disclosure or modification, the TOE can be configured to utilize an IPSEC virtual private network (VPN) to provide AES-based cryptographic protection for this purpose. This protection is initiated by the TOE whenever SYSLOG connections are established for the purpose of exporting audit records. The TOE can be configured to use AES with key sizes of 128, 192 or 256 for IPsec ESP.

All of the secure protocols are supported by the cryptographic operations provided by the FCS requirements in this Security Target.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1: The TOE can be configured to use an IPSEC VPN to ensure that exported audit records are not subject to inappropriate disclosure or modification.
- FTP_TRP.1: The TOE provides SSHv2, based on its embedded cryptomodule, to support secure remote administration. Furthermore, the TOE supports SNMPv3, also based on its embedded cryptomodule, for secure remote non-interactive remote administration functions. In each case, the administrator can initiate the remote session, the remote session is secured (disclosure and modification) using cryptographic operations, and all remote security management functions require the use of one of these secure channels.

7.9 TOE Summary Specification Rationale

Each prior subsection in Section 7, 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 functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 7-2 Security Functions vs. Requirements Mapping demonstrates the relationship between security requirements and security functions.

	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.1a		X						
FCS_CKM.1b		X						

FCS_CKM.4		X						
FCS_COP.1a		X						
FCS_COP.1b		X						
FCS_COP.1c		X						
FDP_IFC.1			X					
FDP_IFF.1			X					
FDP_RIP.2			X					
FIA_AFL.1				X				
FIA_ATD.1				X				
FIA_SOS.1				X				
FIA_UAU.1				X				
FIA_UAU.5				X				
FIA_UID.2				X				
FMT_MOF.1					X			
FMT_MSA.1					X			
FMT_MSA.3					X			
FMT_SMF.1					X			
FMT_SMR.1					X			
FPT_STM.1						X		
FPT_TST.1						X		
FTA_SSL.3							X	
FTA_TAB.1							X	
FTP_ITC.1								X
FTP_TRP.1								X

Table 7-2 Security Functions vs. Requirements Mapping