National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Hewlett-Packard Development Company, L.P., 11445 Compaq Center Drive West, Houston, Texas 77070

Hewlett-Packard Company A-Series Routers

Report Number: CCEVS-VR-10470-2013
Dated: March 20, 2013
Version: 0.2

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Kenneth Stutterheim
Aerospace Corporation
Columbia, MD

Mario Tinto
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Tammy Compton
Chris Keenan
Quang Trinh
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary ... 1
2 Identification ... 2
3 Architectural Information ... 4
3.1 Intelligent Resilient Framework ... 5
3.2 Physical Boundaries ... 6
4 Security Policy ... 6
4.1 Security Audit ... 7
4.2 Cryptographic Support ... 7
4.3 User Data Protection ... 7
4.4 Identification and Authentication ... 7
4.5 Security Management ... 8
4.6 Protection of the TSF ... 8
4.7 Resource utilisation ... 8
4.8 TOE access ... 9
4.9 Trusted path/channels ... 9
5 Assumptions ... 9
6 Documentation ... 10
6.1 Design Documentation ... 10
6.2 Guidance Documentation ... 10
6.3 Life Cycle ... 12
6.4 Testing ... 12
7 IT Product Testing ... 12
7.1 Developer Testing ... 12
7.2 Evaluation Team Independent Testing ... 13
8 Evaluated Configuration ... 13
9 Results of the Evaluation ... 14
9.1 Evaluation of the Security Target (ASE) ... 14
9.2 Evaluation of the Development (ADV) ... 15
9.3 Evaluation of the Guidance Documents (AGD) ... 15
9.4 Evaluation of the Life Cycle Support Activities (ALC) ... 15
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) ... 16
9.6 Vulnerability Assessment Activity (VAN) ... 16
9.7 Summary of Evaluation Results ... 16
10 Validator Comments/Recommendations ... 16
11 Annexes ... 17
12 Security Target ... 17
13 Glossary ... 17
14 Bibliography ... 18

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Hewlett-Packard Company A-Series Routers solution provided by Hewlett-Packard Company. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in September 2012. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.2.

The Hewlett-Packard Company A-Series Router TOE is a stand-alone network router appliance designed to implement a wide range of network layer 2 and 3 services, routing and firewall capabilities. The firewall functionality included within the TOE provides the functionality specified in the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the Hewlett-Packard Company A-Series Routers Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Hewlett-Packard Company A-Series Routers with Comware version 5.20

Product Series	Specific Devices
HP A6600 Series with • HP A6600 Firewall Processing Module	HP A6616 Router Chassis
	HP A6608 Router Chassis
	HP A6604 Router Chassis
HP A8800 Series	HP A8805 Router Chassis

Item	Identifier	
	with • HP A8800 Firewall Processing Module	HP A8808 Router Chassis
		HP A8812 Router Chassis
	HP A-MSR30 Series	HP A-MSR30-20 Multi-service Router
		HP A-MSR30-40 Multi-service Router
		HP A-MSR30-60 Multi-service Router
		HP A-MSR30-20 PoE Multi-service Router
		HP A-MSR30-40 PoE Multi-service Router
		HP A-MSR30-60 PoE Multi-service Router
		HP A-MSR30-10 Router
	HP A-MSR50 Series	HP A-MSR50-40 Multi-service Router
		HP A-MSR50-60 Multi-service Router
		HP A-MSR50-40 DC Multi-service Router
		HP A-MSR50-60 DC Multi-Service Router
Protection Profile	U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007	
ST:	Hewlett-Packard Company A-Series Routers Security Target, Version 1.0, March 20, 2013	
Evaluation Technical Report	Evaluation Technical Report For Hewlett-Packard Company A-Series Routers (Proprietary), Version 3.0, August 17, 2012	
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3	
Conformance Result	CC Part 2 extended, CC Part 3 conformant	
Sponsor	Hewlett-Packard Company	
Developer	Hewlett-Packard Company	
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD	
CCEVS Validators	Kenneth Stutterheim, Aerospace Corporation, Columbia, MD Mario Tinto, Aerospace Corporation, Columbia, MD	

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The HP A-Series routers all share a common software code base, called Comware. Comware is special purpose appliance system software that implements a wide array of networking technology, including: IPv4/IPv6 dual-stacks, a data link layer, Ethernet switching, Intelligent Resilient Framework (IRF), routing, Quality of Service (QoS), etc.. The evaluated version of Comware is 5.2. It should be noted that Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows; however, the only underlying architecture found in the evaluated configuration is Linux.

The Comware v5.2 architecture can be depicted as follows:

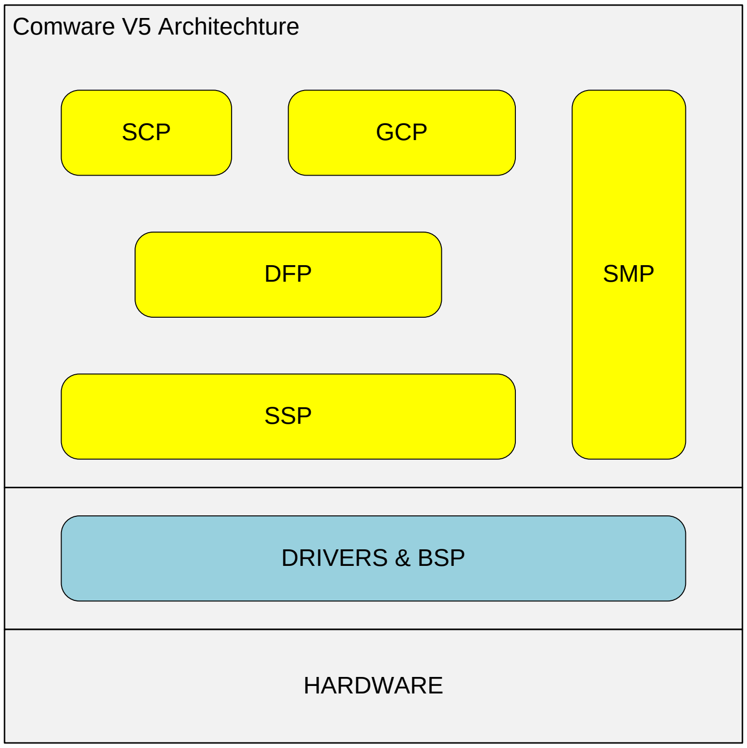

Figure 1 Comware v5.2 Architecture

- ***General Control Plane (GCP)* –** The GCP fully supports the IPv4 and IPv6 protocol stacks and provides support to a variety of IPv4/IPv6 applications including routing protocols, voice, WAN link features, and QoS features.

- ***Service Control Plane (SCP) –*** The SCP supports value-added services such as connection control, user policy management AAA, RADIUS, and TACACS+.
- ***Data Forwarding Plane (DFP) –*** The DFP underpins all network data processing. The forwarding engine is the core of the DFP.
- ***System Management Plane (SMP) –*** The SMP provides user interfaces for device management. This includes implementations for Command line - CLI (SSHv2), Web (HTTPS), and Management Information Base - MIB (SNMPv3) management options.
- ***System Service Plane (SSP) –*** The SSP provides a foundation layer that implements primitives on which the other planes rely, for example, memory management, task management, timer management, message queue management, semaphore management, time management, IPC, RPC, module loading management and component management.

Underlying the main Comware components are the hardware-specific Board Support Package (BSP) and device drivers to provide necessary abstractions of the hardware components for the higher-level software components.

The Comware software components are composed of subsystems designed to implement applicable functions. For example there are subsystems dedicated to MIB, Web, 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 SSH, SNMPv3, and HTTPS (HTTP over TLSv1) and also digital signatures used to protect the available remote management and to enable secure update capabilities of the TOE. Otherwise, the TOE implements a wide range of network switching protocols and functions.

More advanced firewall security features are also available including stateful packet filtering and IPSec VPN 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.

3.1 Intelligent Resilient Framework

As indicated above, multiple HP A-Series switch devices can be deployed as an IRF group. Each device in the IRF group is directly connected to the other IRF group members using an IRF stack utilizing dedicated network connections. One device in the group is designated as master and should that device fail a voting procedure ensues to elect a new master among the remaining IRF group members.

All A-Series devices in the group share the same configuration, which is shared across the IRF connections when the group is formed and later when configuration changes occur.

Management of the IRF group can occur via any of the IRF group members by an authorized administrator.

Once configured the IRF group acts as a single, logical switch with a common configuration and will act to receive and forward network traffic in accordance with that common configuration. When necessary, network traffic is forward through the IRF connection in order to get the network traffic to and from the applicable physical network connections used to attach other network peers or clients.

Note that the IRF connections are not secured (e.g., using encryption) by the TOE, so the IRF group members must necessarily be collocated and the IRF connections need to be as protected as the IRF group devices themselves.

3.2 Physical Boundaries

The TOE is a physical network rack-mountable appliance (or IRF connected group of appliances) 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 list of applicable series and devices is provided in section **Error! Reference source not found.** and the applicable modules for each series are identified in section **Error! Reference source not found.**.

Alternately, the TOE can be deployed as a pair of appliances connected via a dedicated high-availability link so that the pair operates in a redundant manner allowing continued operations should one of the appliances fail.

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.
- Certificate Authority (CA) server – The TOE can be configured to utilize digital certificates, e.g., for VPN and HTTPS connections.
- VPN Peers – The TOE can establish VPNs with peers via IPSec.
- Management Workstation – The TOE supports CLI and Web access and as such an administrator would need a terminal emulator (supporting SSHv2) or web browser (supporting HTTPS) to utilize those administrative interfaces.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Security management
6. Protection of the TSF
7. Resource utilisation
8. TOE access
9. Trusted path/channels

4.1 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 or alternately to send the logs to a designated log server. Locally stored audit records can be reviewed and otherwise managed by an administrator.

4.2 Cryptographic Support

The TOE includes a FIPS 140-2 -certified cryptographic module (Certificate #1911, #1913 and #1914) that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including IPSec, SSH, HTTPS, and SNMP.

4.3 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 stateful packet filtering and IPSec VPNs services. These services can be configured and monitored by an administrator.

4.4 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 (SSHv2 and HTTPS) for interactive administrator sessions. An SNMPv3 interface, which also requires proper user credentials, is also available non-interactive MIB based management of the TOE.

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

4.5 Security Management

The TOE provides Command Line (CLI) commands, a Web-based Graphical User Interface (Web GUI)[1], 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.

4.6 Protection of the TSF

The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

From a communication perspective it employs both dedicated communication channels (based on physically separate networks and VLAN technology) and also cryptographic means (e.g., to prevent replays) to protect communication between distributed TOE components as well as between TOE and other components in the operation environment (e.g., administrator workstations). Note that IRF communication is not considered communication between distributed TOE components, but rather is communication among collocated components that logically form an instance of the TOE. As such, since the IRF communication channels are not protected using mechanisms such as encryption, they need to be as protected as the TOE devices themselves.

The TOE includes functions to perform self-tests at startup so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

4.7 Resource utilisation

The TOE can limit network connections in order to ensure that administrators will be able to connect when they need to perform security management operations on the TOE.

[1] The Web interface is implemented only in the A-MSR30 and A-MSR50 Series routers.

4.8 TOE access

The TOE can be configured to display an informative banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session will be terminated.

4.9 Trusted path/channels

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

The TOE protects communication with network peers, such as a log server, using an IPSec VPNs.

5 Assumptions

The following assumptions were made during the evaluation of Hewlett-Packard Company A-Series Routers:

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- 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.
- There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
- The TOE is physically secure.
- The TOE does not host public data.
- Authorized administrators may access the TOE remotely from the internal and external networks
- Information can not flow among the internal and external networks unless it passes through the TOE

6 Documentation

The following documentation was used as evidence for the evaluation of the Hewlett-Packard Company A-Series Routers:

6.1 Design Documentation

1. Hewlett-Packard Company A-Series Switch and Router Device Design Documentation DRAFT, Revision 0.3, December 9, 2011
2. Comware 5.2 Design, Version 1.07, 2010-06-21

6.2 Guidance Documentation

1. Preparative Procedures for CC EAL2 Evaluated Hewllet-Packard A-Series Family
2. Command Reference for CC Supplement for 6600
3. Command Reference for CC Supplement for MSR 30 and 50
4. Command Reference for CC Supplement for Firewall Modules
5. Configuration Reference for CC Supplement for 6600
6. Configuration Reference for CC Supplement for MSR 30 and 50
7. Configuration Reference for CC Supplement for Firewall Modules
8. H3C SR6600Fundamentals Configuration Guide (Document Version: 20110627-C-1.11)
9. H3C SR6600 Routers Fundamentals Command Reference (Document Version: 20110627-C-1.11)
10. H3C SR6600 Routers Fundamentals Command Reference (Document Version: 20110627-C-1.11)
11. H3C SR6600 Routers ACL and QoS Configuration Guide (Document Version: 20110627-C-1.11)
12. H3C SR6600 Routers ACL and QoS Command Reference (Document Version 20110627-C-1.11)
13. H3C SR6600 Routers Security Configuration Guide (Document Version: 20110627-C-1.11)
14. H3C SR6600 Routers Security Command Reference (Document Version: 20110627-C-1.11)
15. IPSec Guide (2.IPsec Commands.doc and 2.IPsec Configuration.doc)
16. H3C SR6600 Routers Network Management and Monitoring Configuration Guide (Document Version: 20110627-C-1.11)

17. H3C SR6600 Routers Network Management and Monitoring Command Reference (Document Version: 20110627-c-1.11)
18. H3C SR6600 Routers OAA Configuration Guide (Document version: 20110627-C-1.11)
19. H3C SR6600 Routers OAA Command Reference (Document version: 20110627-C-1.11)H3C SR8800 10G Core Routers Fundamentals Configuration Guide (Document Version: 6W102-20110415)
20. H3C SR8800 10G Core Routers Fundamentals Command Reference (Document Version: 6W102-20110415)
21. H3C SR8800 10G Core Routers ACL and QoS Configuration Guide (Document Version: 6W102-20110415)
22. H3C SR8800 10G Core Routers ACL and QoS Command Reference (Document Version: 6W102-20110415)
23. H3C SR8800 10G Core Routers Security Configuration Guide (Document Version: 6W102-20110415)
24. H3C SR8800 10G Core Routers Security Command Reference (Document Version: 6W102-20110415)
25. H3C SR8800 10G Core Routers Network Management and Monitoring Configuration Guide (Document Version: 6W102-20110415)
26. H3C SR8800 10G Core Routers Network Management and Monitoring Command Reference (Document Version: 6W102-20110415)
27. H3C SR8800 10G Core Routers OAA Configuration Guide (Document version: 6W102-20110415)
28. H3C SR8800 10G Core Routers OAA Command Reference (Document version: 6W102-20110415)
29. H3C MSR Series Routers Fundamentals Configuration Guide (Document Version: 20110715-C-1.09)
30. H3C MSR Series Routers Fundamentals Command Reference (Document Version: 20110715-C-1.09)
31. H3C MSR Series Routers ACL and QoS Configuration Guide (Document Version: 20110715-C-1.09)
32. H3C MSR Series Routers ACL and QoS Command Reference (Document Version: 20110715-C-1.09)
33. H3C MSR Series Routers Security Configuration Guide (Document Version: 20110715-C-1.09)
34. H3C MSR Series Routers Security Command Reference (Document Version: 20110715-C-1.09)
35. IPSec Guide (2.IPsec Commands.doc and 2.IPsec Configuration.doc)

36. H3C MSR Series Routers Network Management and Monitoring Configuration Guide (Document Version: 20110715-C-1.09)
37. H3C MSR Series Routers Network Management and Monitoring Command Reference (document Version: 20110715-C-1.09)
38. H3C MSR Series Routers OAA Configuration Guide (Document version: 20110715-C-1.09)
39. H3C MSR Series Routers OAA Command Reference (Document version: 20110715-C-1.09)
40. H3C SecPath Series High-End Firewalls Getting Started Guide (Document version: 5PW105-20110921)
41. H3C SecPath Series High-End Firewalls Access Control Configuration Guide (Document version: 5PW105-20110921)
42. H3C SecPath Series High-End Firewalls VPN Configuration Guide (Document version: 5PW105-20110921)
43. H3C SecPath Series High-End Firewalls System Management and Maintenance Configuration Guide (Document version: 5PW105-20110921)

6.3 Life Cycle

1. Hewlett-Packard Company A-Series Life Cycle Document, Revision 0.1, August 30, 2011

6.4 Testing

1. Test Documentation For H3C Series Routers running Comware V5.2, version V1.01, 2012-02-15

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Hewlett-Packard Company A-Series Routers, Version 3.0, August 17, 2012.

7.1 Developer Testing

At EAL2, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing addressed each of the security functions identified in the ST and interfaces in the design. These security functions include:

- Security audit
- Cryptographic support
- User data protection

- Identification and authentication
- Security management
- Protection of the TSF
- Resource utilisation
- TOE access
- Trusted path/channels

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Preparative Procedures for CC EAL2 Evaluated Hewlett-Packard A-Series Family, ran a the entire vendor test suite and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The evaluation team testing focused on testing boundary conditions not tested by HP. For vulnerability testing the evaluation team performed port and vulnerability scanning as well as other team developed tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Hewlett-Packard Company A-Series Routers including:

- Hewlett-Packard Company A-Series Switches with Comware version 5.20

Product Series	Specific Devices
HP A6600 Series with • HP A6600 Firewall Processing Module	HP A6616 Router Chassis
	HP A6608 Router Chassis
	HP A6604 Router Chassis
HP A8800 Series with • HP A8800 Firewall Processing Module	HP A8805 Router Chassis
	HP A8808 Router Chassis
	HP A8812 Router Chassis
HP A-MSR30 Series	HP A-MSR30-20 Multi-service Router
	HP A-MSR30-40 Multi-service Router
	HP A-MSR30-60 Multi-service Router
	HP A-MSR30-20 PoE Multi-service Router

Product Series	Specific Devices
	HP A-MSR30-40 PoE Multi-service Router
	HP A-MSR30-60 PoE Multi-service Router
	HP A-MSR30-10 Router
HP A-MSR50 Series	HP A-MSR50-40 Multi-service Router
	HP A-MSR50-60 Multi-service Router
	HP A-MSR50-40 DC Multi-service Router
	HP A-MSR50-60 DC Multi-Service Router

To use the product in the evaluated configuration, the product must be configured as specified in the **Preparative Procedures for CC EAL2 Evaluated Hewlett-Packard A-Series Family** document.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL2 augmented with ALC_FLR.2 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 3 and CEM version 3.1 rev 3. The evaluation determined the Hewlett-Packard Company A-Series Routers TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Hewlett-Packard Company A-Series Routers product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 2 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation.

In addition to the EAL 2 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 2 VAN CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the entire vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team considers the evaluated subset of product functions to be consistent with the product's intended purpose and mode of operation. The rationale for excluded features is plausible and introduces no unreasonable constraints.

The evaluation team observed that the vendor's security tests are predominantly manual and apparently not closely integrated with the extensive automated testing performed as a routine part of product development. While these evaluated tests are sufficient to satisfy

Common Criteria requirements, the validation team recommends a closer integration in future efforts, in order to improve test integration and provide greater test coverage.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Hewlett-Packard Company A-Series Routers Security Target, Version 1.0, March 20, 2013*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Science Applications International Corporation. *Evaluation Technical Report for the Hewlett-Packard Company A-Series Routers Part 2 (Proprietary),* Version 3.0, August 17, 2012.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Hewlett-Packard Company A-Series Routers*, *ETR Part 2 Supplement (SAIC and HP Proprietary),* Version 3.0, August 17, 2012.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Hewlett-Packard Company A-Series Routers Security Target, Version 1.0, March 20, 2013