National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Dell Networking Platforms running Dell Networking OS v9.6

Report Number: **CCEVS-VR-VID10588-2015**
Dated: **March 19, 2015**
Version: **1.0**

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 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mr. Paul Bicknell

The MITRE Corporation

Bedford, MA

Mr. Daniel Faigin

The Aerospace Corporation

Los Angeles, CA

Mr. Chris Thorpe

The MITRE Corporation

McLean, VA

Common Criteria Testing Laboratory

Mr. Herb Markle

Mr. Iain Holness

CygnaCom Solutions

McLean, Virginia

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the Dell Networking Switches Security Target.

Table of Contents

List of Figures and Tables

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the Dell Networking Platforms running Dell Networking OS v9.6 as defined in the *Dell Networking Switches Security Target v1.0.*

The evaluated Dell Networking Platforms running Dell Networking OS v9.6 consists of S4810, S4820T, S5000, S6000 top-of-rack data center switches, and Z9000, Z9500 end-of-row data center switches. The TOE provides layer 2 and 3 network management and interconnectivity functionality by offering non-blocking, line-rate Ethernet switching with Quality of Service (QoS) and a full complement of IPv4 and IPv6 features. TOE consists of a hardware appliance with embedded software components.

The Target of Evaluation (TOE) is a Network Device as defined by the *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1: "*A network device is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise".*

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in January 2015. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is:

- Common Criteria version 3.1 R4 Part 2 extended and Part 3 conformant
- Demonstrates exact compliance to *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 as changed/clarified by *Security Requirements for Network Devices Errata #3 and all applicable Technical Decisions*.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org.

2. Identification

Target of Evaluation: Dell Networking Platforms running Dell Networking OS v9.6

Platform	Model	Processor	Form	Specs
Dell Networking S-Series Switches	S4810	Power Architecture e500 Series	1U Top-of-rack	48x 10G SFP+ 4x 40GbE QSFP+
	S4820T	Power Architecture e500 Series	1U Top-of-rack	48 x 1/10G BASE-T 4 x 40GbE QSFP+
	S5000	2 x Power Architecture e500 Series	1U Top-of-rack	4x40GbE QSFP+ 4 module bays with: 0-4 12x 10G SFP+ or 0-1 12 2/4/8Gbps FC modules
	S6000	Atom Centerton Series	1U Top-of-rack	32x 40GbE QSFP+
Dell Networking Z-Series Switches	Z9000	Xeon C5500 Series	2U End-of-row	32x 40GbE QSFP+
	Z9500	5 x Atom Centerton Series	3U End-of-row	132x 40GbE QSFP+

Developer: Dell USA L.P.

CCTL: CygnaCom Solutions
7925 Jones Branch Dr, Suite 5400
McLean, VA 22102-3321

Evaluators: Herb Markle
Iain Holness

Validation Scheme: National Information Assurance Partnership
CCEVS

Validators: Paul A. Bicknell, Daniel Faigin, Chris Thorpe

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1 R4, Sept 2012

CEM Identification: Common Methodology for Information Technology Security Evaluation, Version 3.1 R4, Sept 2012

3. Security Policy

The TOE enforces the following security policies as described in the ST:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted path/Channel

3.1. Security Audit

The TOE generates audit records for all security-relevant events. For each event, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event logged. The resulting logs can be stored locally to be viewed by an administrator or securely sent to a designated syslog server for archiving. The logs can be viewed by administrators using the appropriate CLI commands. The TOE also implements timestamps to ensure reliable audit information is available.

3.2. Cryptographic Support

The TOE performs the following cryptographic operations:

- Secure channel with following parameters:
  - AES128-CBC, AES256-CBC for data encryption
  - RSA for host key algorithm
  - HMAC-SHA1, HMAC-SHA1-96, HMAC-SHA2-256 for data integrity
  - diffie-hellman-group14-sha1 for key exchange
- Random Bit Generation using CTR-DRBG (AES-256)
- Critical Security Parameters (CSPs) zeroization

The TOE uses a dedicated cryptographic module to manage CSPs and implements zeroization procedures to mitigate the possibility of disclosure or modification of CSPs. Additionally, the TOE provides commands to on-demand zeroize CSPs (e.g. host RSA keys), that can be invoked by an authorized administrator with appropriate permissions.

3.3. User Data Protection

The TOE implements multiple measures to ensure residual information is not transmitted. Ingress packets are stored in the managed buffer that allocates dedicated memory space

of the exact size required. Once the packet has been either transmitted or discarded, the memory used for that packet is returned back to the pool for reuse.

3.4. Identification and Authentication

The TOE supports Role-Based Access Control (RBAC) managed by an AAA module that stores and manages permissions of all users and their roles. Before any other action, each user is identified with a login name and authenticated with a password. Each authorized user is associated with assigned role and specific permissions that determine access to TOE features. The AAA module stores the assigned role of each user along with all other information required that user to access the TOE.

3.5. Security Management

The TOE allows remote administration using an SSHv2 session over an out of band LAN management RJ-45 port and local administration using a console via a separate RJ-45 running RS-232 signaling/USB port. Both remote and local administration conducted over command-line interface (CLI) terminal that facilitates access to all management functions used to administer the TOE.

All of the management functions are restricted to the authorized administrators of the TOE. Authorized administrators can perform the following actions: manage user accounts and roles, reboot and apply software updates, administer system configuration, and review the audit records.

The term “authorized administrator” is used to refer to any administrative user with the appropriate role to perform the relevant functions.

3.6. Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features.

The TOE protects CSPs, including stored passwords and cryptographic keys, so they are not directly viewable in plaintext. The TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment.

The TOE employs both dedicated communication channels as well as cryptographic means to protect communication between itself and other components in the operational environment.

The TOE performs self-tests to detect internal failures and protect itself from malicious updates.

3.7. TOE Access

The TOE will display a customizable banner when an administrator initiates an interactive local or remote session. The TOE also enforces an administrator-defined inactivity timeout after which the inactive session is automatically terminated. Once a

session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

3.8. Trusted Path/Channels

The TOE protects remote sessions by establishing a trusted path between itself and the administrator. The TOE prevents disclosure or modification of logs by establishing a trusted channel between itself and the Syslog server. To implement trusted path/secure channel the TOE uses an SSHv2 protocol with password-based or public key-based authentication.

3.9. Secure Usage Assumptions

The ST identifies the following assumptions about the use of the product:

1. 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. The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
2. Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
3. TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4. Architectural Information

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, and processor and software that implements routing and switching functions, configuration information and drivers. While hardware varies between different appliance models, the software (Dell Networking OS v9.6) is shared across all platforms.

Dell Networking OS v9.6 is composed of subsystems designed to implement operational, security, management, and networking functions. Hardware-specific device drivers that reside in the kernel provide abstraction of the hardware components. Dedicated cryptographic module provides functionality that implements secure channel and protects critical security parameters. Control plane subsystem that includes Internet Protocol (IP) host stack, which can be further subdivided into protocol and control layers, implements switching and routing functions. System management subsystem, that includes an Authentication, Authorization and Accounting (AAA) module, implements administrative interface and maintains configuration information.

The physical boundary of the TOE is the Dell Networking Platforms running Dell Networking OS v9.6**,** which includes:

- The appliance hardware
    - RJ-45/RS-232 management ports
    - USB management port (except S4810 model)
    - Dedicated Ethernet management port
- Embedded software installed on the appliance
    - CLI management interface

The Operational Environment of the TOE includes:

- The SSH client that is used to remotely access the management interface
- The management workstation that hosts the SSH client
- Optional external IT servers:
    - Syslog for external storage of audit logs
    - NTP for synchronizing system time

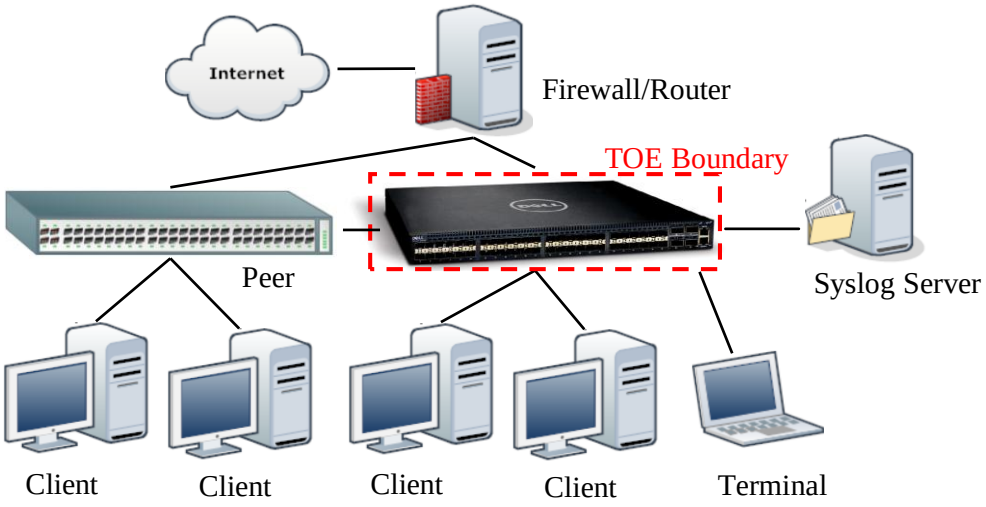

Figure 1: TOE Boundary

The TOE supports a number of features that are not part of the core functionality. These features are not included in the scope of the evaluation:

- Any integration and/or communication with authentication servers such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control Systems (TACACS) is excluded from the evaluated configuration.
- Remote management using web interface (Secure HTTP or HTTPS) is excluded. The TOE does not satisfy all NDPP requirements for this administrative interface and it is disabled in the evaluated configuration.
- Routing protocols that integrate authentication or encryption such as Routing Information Protocol (RIPv1, RIPv2), Open Shortest Path First (OSPFv2), Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), and Virtual Router Redundancy Protocol (VRRP), due to RFC-compliant implementations, are unable to satisfy NDPP cryptographic requirements.
- Use of the FTP server is excluded and it is disabled by default.
- Use of the SNMP functionality is excluded and it is disabled by default. The use of SNMPv3 is not restricted; however, it is an excluded function in NDPP evaluations.

5. Documentation

The following documents were available for the evaluation. These documents are developed and maintained by Dell and delivered to the end user of the TOE:

5.1. Security Target

Dell Networking Switches Security Target, Version 1.0, January 22, 2015

5.2. User Documentation

Reference Title Based on Model
Dell Command Line Reference Guide for the S4810 System, September 23 2014 *Dell Configuration Guide for the S4810 System, September 23 2014* *Dell Release Notes for the S4810 System, Dell Networking OS v9.6, September 2014*
Dell Command Line Reference Guide for the S4820T System, September 23 2014 *Dell Configuration Guide for the S4820T System, September 23 2014* *Dell Release Notes for the S4820T System, Dell Networking OS v9.6, September 2014*
Dell Command Line Reference Guide for the S5000 System, September 23 2014 *Dell Configuration Guide for the S5000 System, September 23 2014* *Dell Release Notes for the S5000 System, Dell Networking OS v9.6, September 2014*
Dell Command Line Reference Guide for the S6000 System, September 23 2014 *Dell Configuration Guide for the S6000 System, September 23 2014* *Dell Release Notes for the S6000 System, Dell Networking OS v9.6, September 2014*
Dell Command Line Reference Guide for the Z9000 System, September 23 2014 *Dell Configuration Guide for the Z9000 System, September 23 2014* *Dell Release Notes for the Z9000 System, Dell Networking OS v9.6, September 2014*
Dell Command Line Reference Guide for the Z9500 System, September 23 2014 *Dell Configuration Guide for the Z9500 System, June September 23 2014* *Dell Release Notes for the Z9500 System, Dell Networking OS v9.6, September 2014*
CC Addendum applicable to all models
Dell Common Criteria Addendum Guide, Dell Networking OS v9.6, January 2015

6. IT Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Evaluator Test Report for Dell Networking Switches* document. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

6.1. Developer Testing

NDPP evaluations do not require developer-testing evidence for assurance activities.

6.2. Evaluator Independent Testing

A test plan was developed in accordance with the Testing Assurance Activities specified in the NDPPv1.1 with Errata 3.

Testing was conducted December 2 to 4, 2014 at the Dell Santa Clara facility at 5450 Great America Parkway, Santa Clara, CA 95054.

The Evaluation Team successfully performed the following activities during independent testing:

- Placed TOE into evaluated configuration by executing the preparative procedures
- Successfully executed the NDPP Assurance-defined tests including the optional SSH tests
- Planned and executed a series of vulnerability/penetration tests

It was determined after examining the Test Report and full set of test results provided by the evaluators the testing requirements for NDPPv1.1 with Errata #3 are fulfilled.

7. Evaluated Configuration

The evaluated version of the TOE is the Dell Networking Platforms running Dell Networking OS v9.6, that in the evaluated configuration consists of S4810, S4820T, S5000, S6000 top-of-rack data center switches, and Z9000, Z9500 end-of-row data center switches, as well as the supporting guidance documentation identified in Section 5.2

8. Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.

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 version 3.1 R4 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Protection Profile *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 with Errata 3.

The evaluation determined the TOE meets the SARs contained the PP.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL (proprietary).

Below are the assurance requirements against which the TOE was required to be evaluated at Evaluation Assurance Level 1. All assurance activities and work units received a passing verdict. The following components are taken from CC part 3:

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.1 Labelling of the TOE
- ALC_CMS.1 TOE CM coverage
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.1 Security objectives
- ASE_REQ.1 Derived security requirements
- ASE_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability survey

The evaluators concluded that the overall evaluation result for the target of evaluation is PASS. The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

8.1. Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

9. Validators Comments/Recommendations

The validators were satisfied with the evaluation team's evaluation and testing efforts. The validators did not identify any gaps or missing information.

The Validators note that administrative diligence in monitoring the SSH-reverse connection is highly recommended. If the connection is dropped, the syslog messages will not be offloaded to the syslog server. When the connection is re-established there is no reconciling the differences between the syslog server and the online audit records. Syslog messages will start transmitting with any new events as they happen. If the connection is down for an extended period of time, the online copy of the audit log could have cycled overwriting audit records that have not been off loaded to the syslog server.

The Validators also note that the TOE supports multiple booting partitions that are very helpful during disaster recovery and is a typical design of network routers/switches. However, the TOE does not warn when system reboot would result in loading different system version than what is presently running.

10. Glossary

10.1. Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

BGP	Border Gateway Protocol
CLI	Command Line Interface
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
IP	Internet Protocol
IPS	Intrusion Protection System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OSPFv2	Open Shortest Path First
PDF	Portable Document Format
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell Network Protocol
SSL	Secure Sockets Layer,
ST	Security Target
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security,
UDP	User Datagram Protocol
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

11. Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009 Version 3.1 Revision 4 Final, CCMB-2012-09-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009 Version 3.1 Revision 4 Final, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, Version 3.1 Revision 4 Final, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, July 2009, Version 3.1 Revision 4 Final, CCMB-2012-09-004.

[5] Protection Profile for Network Devices, 08 June 2012. Version 1.1

[6] Security Requirements for Network Devices, Errata #3, 3 November 2014