National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Dell Networking Platforms running Dell EMC Networking OS 9.14

Report Number: **CCEVS-VR-VID11049**
Dated: **December 10, 2019**
Version: **0.5 Draft**

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Paul A. Bicknell

Jenn Dotson

Randy Heimann

Lisa Mitchell

Chris Thorpe

The MITRE Corporation

Bedford, MA

Common Criteria Testing Laboratory

Fathi Nasraoui

Kirill Sinitski

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 Platforms 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 EMC Networking OS 9.14.1.9 as defined in the *Dell Networking Platforms Security Target v2.9.*

The TOE is the Dell Networking Platforms running Dell EMC Networking OS 9.14(1.9) which in the evaluated configuration consists of S-Series, C-Series, and Z-Series 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). TOE consists of a hardware appliance with embedded software components.

The TOE is a Network Device as defined by the *collaborative Protection Profile for Network Devices v2.1* [NDcPP]: "*A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network".*

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in October 2019. 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 R5 Part 2 and Part 3 conformant,
- and demonstrates exact conformance to *collaborative Protection Profile for Network Devices, Version 2.1, September 2018* as clarified by 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.

The Validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associate test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the Security Target (ST). The validation team, therefore, concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

2. Identification

Target of Evaluation: Dell Networking Platforms running Dell EMC Networking OS 9.14

Platform	Model	Processor	Form	Specs
Dell Networking S-Series Switches	S3124	ARM Cortex A9	1U	24 x 1000BASE-T
	S3124P	ARM Cortex A9	1U	24 x 1000BASE-T PoE+
	S3124F	ARM Cortex A9	1U	24 x 1GbE SFP
	S3148	ARM Cortex A9	1U	48 x 1000BASE-T
	S3148P	ARM Cortex A9	1U	48 x 1000BASE-T PoE+
	S3048-ON	Intel Atom C Series	1U	48 x 100BASE-T 4 x 1-GbE SFP+
	S4048-ON	Intel Atom C Series	1U	48 x 10GbE SFP+ 6 x 40GbE QSFP+
	S4048T-ON	Intel Atom C Series	1U	48 x 10GBASE-T 6 x 40GbE QSFP+
	S5048F-ON	Intel Atom C Series	1U	72 x 25GbE or 48 x 25GbE 6 x 100 GbE
	S6010-ON	Intel Atom C Series	1U	32 x 40GbE QSFP+
	S6100-ON	Intel Atom C Series	2U	2 x 10GbE SFP+ 4 module bays with: 16 x QSFP+ 40GbE or 8 x QSFP28 100GbE
Dell Networking C-Series Switches	C9010 and C1048P port extender	Intel Atom C Series	8U	10 module bays with: 24-port 10GbE 10GBASE-T Line Card or 24-port 10GbE SFP+ or 6-port 40GbE QSFP+
Dell Networking Z-Series Switches	Z9100-ON	Intel Atom C Series	1U	32 x 100GbE QSFP28 or 64 x 50GbE QSFP+ or 32 x 40GbE QSFP+ or 128 x 25GbE QSFP+ or 128 x 25GbE QSFP+ 2 x 10GbE

Developer: Dell USA L.P.

CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5400 McLean, VA 22102-3321
Evaluators:	Fathi Nasraoui Kirill Sinitski
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Paul A. Bicknell, Jenn Dotson, Randy Heimann, Lisa Mitchell, Chris Thorpe
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

3. Security Policy

The TOE enforces the following security policies as described in the Security Target (ST):

- Security Audit
- Cryptographic Support
- 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 records can be stored locally or securely sent to a designated audit server for archiving. Security Administrators using the appropriate CLI commands can also view audit records locally. The TOE also implements timestamps to ensure reliable audit information produced.

3.2. Cryptographic Support

The TOE performs the following cryptographic functionality:

- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification utilizing dedicated cryptographic library
- Cryptographic functionality is utilized to implement secure channels
  - SSHv2
  - TLSv1.2
- Entropy is collected and used to support seeding with full entropy
- Critical Security Parameters (CSPs) internally stored and cleared when no longer in use
- X509 Certificate authentication integrated with TLS protocol

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

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. 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.

3.4. 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 Security Administrators of the TOE. Security 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.

3.5. 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.

The TOE implements NTPv4 to synchronize time with NTP timeserver. The use of keyed-SHA1 cryptographic authentication and a robust trusted key provide for reliable means of exchanging NTP packets with trusted time sources.

3.6. 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 administrator to re-authenticate.

3.7. 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.

3.8. Secure Usage Assumptions and Clarification of Scope

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. TOE Administrators are expected to fully validate any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE’s trust store prior to use
5. The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
6. The administrator’s credentials used to access the network device are protected.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 NDcPPv2.1 and performed by the evaluation team).

2. This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
3. 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.
4. The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPPv2.1 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

4. Architectural Information

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, processor and software that implements routing and switching functions, configuration information and drivers. While hardware varies between different appliance models, the software (Dell EMC Networking OS v9.14) is shared across all platforms.

Dell EMC Networking OS v9.14 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 is integrated with protocol libraries that implement secure channel functionality. 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 includes:

- The appliance hardware
  - RJ-45/RS-232 management ports
  - USB port
  - 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
- External IT servers:
  - Audit server for external storage of audit records
  - NTP server for synchronizing system time
  - Certificate Authority and OCSP servers to support X.509 (optional)

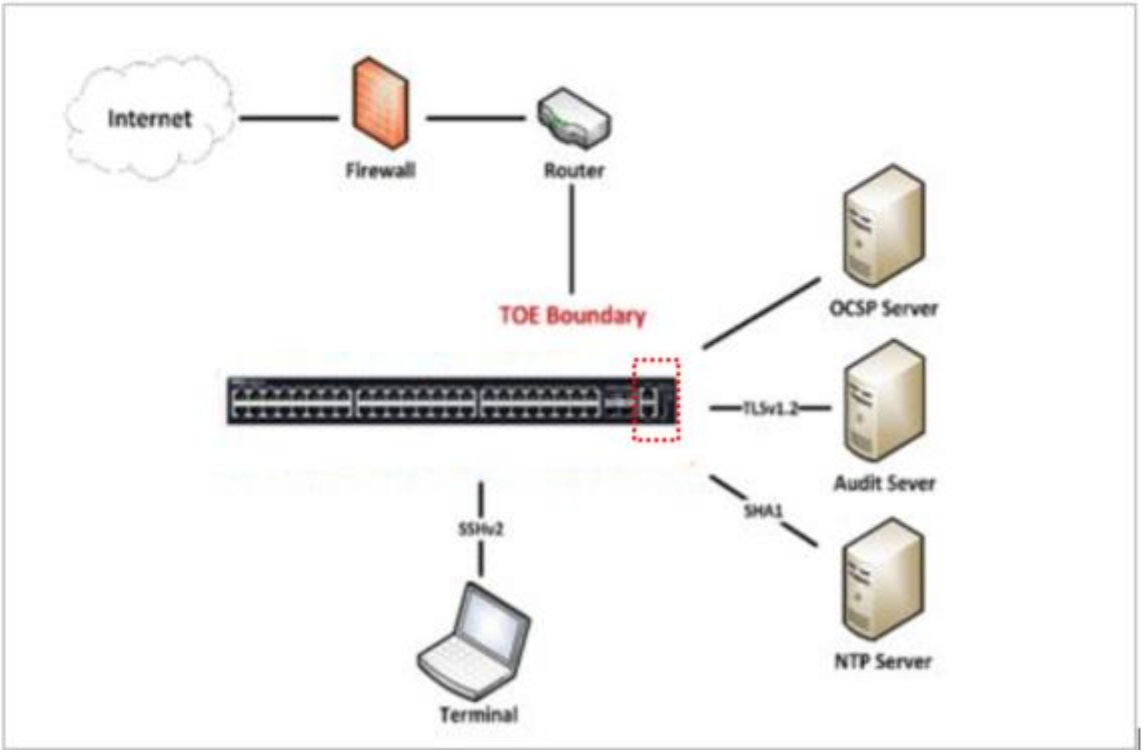

Figure 1: TOE Boundary

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.
- Any use of HTTP and HTTPS (web interface) or OpenManage Network Manager (ONM) is excluded and are 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) are not evaluated. RFC-compliant implementations are unable to satisfy cryptographic requirements outlined in the PP.
- Use of the FTP server is excluded and it is disabled by default.
- Use of the SNMP management functionality is excluded and it is disabled by default. The use of SNMPv3 for monitoring is not restricted; however, it is not evaluated.
- Reverse SSH tunnel with syslog is excluded from the evaluated configuration.

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 Platforms Security Target, Version 2.9, December 02, 2019

5.2. *User Documentation*

Reference Title	ID
Dell Configuration Guide for the S6010-ON System 9.14.1.0 Dell Configuration Guide for the S6100-ON System 9.14.1.0 Dell Configuration Guide for the S5048F-ON System 9.14.1.0 Dell Configuration Guide for the S4048-ON System 9.14.1.0 Dell Configuration Guide for the S3100-ON System 9.14.1.0	[ADMIN]
Dell Networking Command Line Reference Guide for the Z9100-ON System 9.14.1.0 Dell Networking Command Line Reference Guide for the C9010 System 9.14.1.0 Dell Networking Command Line Reference Guide for the S3048-ON System 9.14.1.0 Dell Command Line Reference Guide for the S6100-ON System 9.14.1.0 Dell Command Line Reference Guide for the S6010-ON System 9.14.1.0 Dell Command Line Reference Guide for the S5048F-ON System 9.14.1.0 Dell Command Line Reference Guide for the S4048-ON System 9.14.1.0 Dell Command Line Reference Guide for the S3100-ON System 9.14.1.0	[REF]
Configuration for Common Criteria NDcPP version 2.1 1 Dell Networking Platforms running Dell EMC Networking OS 9.14.1	[CC Addendum]

6. IT Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Test Report for Dell Networking Platforms* 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

NDcPPv2.1 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 NDcPPv2.1.

Testing was conducted October 10-30 at the Cygnacom Lab at 1000 Innovation Drive, ON, Canada K2K 3E7.

The Evaluator successfully performed the following activities during independent testing:

- Placed TOE into evaluated configuration by following the preparative procedures
- Successfully executed the NDcPP Assurance-defined tests including the selection-based SSH, TLS, and X509 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 NDcPPv2.1 are fulfilled.

7. 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 (CC), Version 3.1 Revision 5. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5.

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 R5 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Protection Profile *collaborative Protection Profile for Network Devices Version 2.1.*

The evaluation determined the TOE meets the SARs contained the NDcPPv2.1.

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

Below lists the security assurance requirements the TOE was required to be evaluated conforming to the NDcPP. All assurance activities and work units received a passing verdict.

- 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. Validators Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Configuration for Common Criteria Guide. No other versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other product functionality included, such as the traffic bearing ports, was not assessed as part of this evaluation. Additional functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

9. Glossary

9.1. Acronyms

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

BGP	Border Gateway Protocol
CEM	Common Evaluation Methodology
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

10. 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 5, CCMB-2017-04-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017 Version 3.1 Revision 5, CCMB-2017-04-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, April 2017, Version 3.1 Revision 5, CCMB-2017-04-004.