National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

AhnLab MDS, MDS with MTA, and MDS Manager V2.1

Report Number: CCEVS-VR-VID10818-2017
Dated: May 8, 2017
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 20755-6940

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of AhnLab MDS, MDS with MTA, and MDS Manager V2.1. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the AhnLab MDS, MDS with MTA, and MDS Manager V2.1 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in May 2017. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in the following Protection Profile:

collaborative Protection Profile for Network Devices Version 1.0, 27 February 2015, [NDcPP] and including the following optional SFRs: FAU_STG.1, FCS_HTTPS_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.2, and FCS_TLSS_EXT.1.

- The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:
    - TD0090: NIT Technical Decision for FMT_SMF.1.1 Requirement in NDcPP
    - TD0094: NIT Technical Decision for validating a published hash in NDcPP
    - TD0095: NIT Technical Interpretations regarding audit, random bit generation, and entropy in NDcPP
    - TD0111: NIT Technical Decision for third party libraries and FCS_CKM.1 in NDcPP and FWcPP
    - TD0112: NIT Technical Decision for TLS testing in the NDcPP v1.0 and FW cPP v1.0.
    - TD0113: NIT Technical Decision for testing and trusted updates in the NDcPP v1.0 and FW cPP v1.0
    - TD0114: NIT Technical Decision for Re-Use of FIPS test results in NDcPP and FWcPP
    - TD0115: NIT Technical Decision for Transport mode and tunnel mode in IPsec communication in NDcPP and FWcPP
    - TD0116: NIT Technical Decision for a Typo in reference to RSASSA-PKCS1v1_5 in NDcPP and FWcPP
    - TD0117 (supercedes TD0093): NIT Technical Decision for FIA_X509_EXT.1.1 Requirement in NDcPP
    - TD0125: NIT Technical Decision for Checking validity of peer certificates for HTTPS servers

- TD0126: NIT Technical Decision for TLS Mutual Authentication
- TD0130: NIT Technical Decision for Requirements for Destruction of Cryptographic Keys
- TD0143: NIT Technical Decision for Failure testing for TLS session establishment in NDcPP and FWcPP
- TD0150: NIT Technical Decision for Removal of SSH re-key audit events in the NDcPP v1.0 and FW cPP v1.0
- TD0151: NIT Technical Decision for FCS_TLSS_EXT Testing - Issue 1 in NDcPP v1.0.
- TD0152: NIT Technical Decision for Reference identifiers for TLS in the NDcPP v1.0 and FW cPP v1.0
- TD0153: NIT Technical Decision for Auditing of NTP Time Changes in the NDcPP v1.0 and FW cPP v1.0
- TD0154: NIT Technical Decision for Versions of TOE Software in the NDcPP v1.0 and FW cPP v1.0
- TD0155: NIT Technical Decision for TLSS tests using ECDHE in the NDcPP v1.0.
- TD0156: NIT Technical Decision for SSL/TLS Version Testing in the NDcPP v1.0 and FW cPP v1.0
- TD0160: NIT Technical Decision for Transport mode and tunnel mode in IPSEC communications
- TD0164: NIT Technical Decision for Negative testing for additional ciphers for SSH
- TD0165: NIT Technical Decision for Sending the ServerKeyExchange message when using RSA
- TD0167: NIT Technical Decision for Testing SSH 2^28 packets
- TD0168: NIT Technical Decision for Mandatory requirement for CSR generation
- TD0169: NIT Technical Decision for Compliance to RFC5759 and RFC5280 for using CRLs
- TD0170: NIT Technical Decision for SNMPv3 Support
- TD0181: NIT Technical Decision for Self-testing of integrity of firmware and software
- TD0182: NIT Technical Decision for Handling of X.509 certificates related to ssh-rsa and remote comms
- TD0183: NIT Technical Decision for Use of the Supporting Document
- TD0184: NIT Technical Decision for Mandatory use of X.509 certificates
- TD0185: NIT Technical Decision for Channel for Secure Update
- TD0186: NIT Technical Decision for Applicability of X.509 certificate testing to IPsec
- TD0187: NIT Technical Decision for Clarifying FIA_X509_EXT.1 test 1
- TD0188: NIT Technical Decision for Optional use of X.509 certificates for digital signatures

- TD0189: NIT Technical Decision for SSH Server Encryption Algorithms
- TD0191: NIT Technical Decision for Using secp521r1 for TLS communication
- TD0195: NIT Technical Decision Making DH Group 14 optional in FCS_IPSEC_EXT.1.1

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

The Leidos evaluation team determined that the AhnLab MDS, MDS with MTA, and MDS Manager V2.1 is conformant to the claimed Protection Profiles (PPs) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and the associated test report produced by the Leidos evaluation team.

The Target of Evaluation (TOE) is a software solution that consists of the AhnLab MDS, MDS with MTA, and MDS Manager V2.1 is a network device that mitigates Advanced Persistent Threat (APT) attacks by identifying known and unknown malware, detecting suspicious traffic, and removing the detected threats. The AhnLab MDS is a malware detection system that inspects network traffic and initiates intrusion mitigation. It is not a network communication filtering device (i.e., not a firewall).

The TOE consists of the following appliances: MDS, or MDS with MTA, or MDS Manager and the software installed on the appliance. Each TOE instance consists of a single appliance and is capable of providing all security functions specified in [NDcPP].

Table 1: TOE Components

Product Series	Specific Product Device	Device Software
MDS	MDS 1000	MDS Analyzer: 2.1.8.25 Data Viewer: 2.1.8.25 Host Controller 2.1.7.22
	MDS 2000	
	MDS 6000	
	MDS10000	
MDS with MTA	MDS 6000	MDS Analyzer: 2.1.8.25 Data Viewer: 2.1.8.25 Host Controller 2.1.7.22
	MDS 10000	
MDS Manager	MDS Manager 2000	Data Viewer: 2.1.8.25 Host Controller: 2.1.7.22
	MDS Manager 5000R	
	MDS Manager 10000R	

The network on which it resides is considered part of the operational environment.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the 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.

Table 2: Evaluation Details

Item	Identifier
Evaluated Product	AhnLab MDS, MDS with MTA, and MDS Manager V2.1
Sponsor & Developer	AhnLab 673 Sampyeong-dong, Bundang-gu, Seongnam-si, Gyeonggi-do, 463-400 Korea
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	May 8, 2017
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
Protection Profiles	*collaborative Protection Profile for Network Devices* Version 1.0, 27 February 2015, [NDcPP] and including the following optional SFRs: FAU_STG.1, FCS_HTTPS_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.2, and FCS_TLSS_EXT.1
Disclaimer	The information contained in this Validation Report is not an endorsement either expressed or implied of the AhnLab MDS, MDS with MTA, and MDS Manager V2.1
Evaluation Personnel	Greg Beaver Cody Cummins Thibaut Marconnet Zalman Kuperman
Validation Personnel	Paul Bicknell Patrick Mallett, PhD Linda Morrison

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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) 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 Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

Table 3: ST and TOE Identification

Name	Description
ST Title	AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Security Target
ST Version	0.3
Publication Date	April 26, 2017
Vendor	AhnLab, Inc.
ST Author	Leidos
TOE Reference	AhnLab MDS, MDS with MTA, and MDS Manager V2.1
TOE Software Version	AhnLab MDS, MDS with MTA, and MDS Manager V2.1
Keywords	Network Device, Malware Detection, Advanced Persistent Threat

3 Architectural Information

The TOE is comprised of one instance of the following product series appliances with software:

- MDS Series Appliance
- MDS with MTA Series Appliance
- MDS Manager Series Appliance

The specific device models and software for each series are identified in Section 1.

Each appliance includes a MDS Manager software component that monitors and responds to malware and abnormal traffic detected by the MDS Analyzer component (described below). The MDS Manager software component has two parts: a Data Viewer and a Host Controller. The Data Viewer records and displays logs and warnings about detected malware files and security events. The Data Viewer observes the abnormal patterns of files and network traffic transferred through the host systems within the internal network, which are logically connected to the MDS system, and controlled directly by Host Controller. The Host Controller runs threat scans and remediation commands on host systems. The Host Controller receives the commands for responding to the malware, based on the administrator's settings, and also communicates with the external MDS agent (when configured) for remediation of detected threats. MDS Agents are not included in the evaluated configuration.

The MDS Manager software component included in all appliances provide all of the security functions specified in the [NDcPP]: identification and authentication of administrators, auditing of security-relevant events, ability to verify the source and integrity of updates to the TOE, protected communications for administration and TOE operation, and specifies CAVP-validated cryptographic mechanisms using OpenSSL-FIPS 2.0.12.

The MDS and MDS with MTA appliances also contain the MDS Analyzer component that detects and analyzes known and unknown malicious files. The MDS Analyzer is located within the network such that it can monitor all of the network traffic. All traffic monitored by the MDS Analyzer is scanned and detected malware causes a notification to be sent to the MDS Manager software component. The MDS Analyzer does not provide any security functionality defined in this ST. The MDS with MTA appliance also consists of MTA functionality available through purchase of a separate license.

In summary, the TOE appliances are network devices composed of the following software components:

- MDS Appliance: MDS Manager software component, and MDS Analyzer component
- MDS with MTA Appliance: MDS Manager software component, MDS Analyzer component, and license to activate the MTA functionality.
- MDS Manager Appliance: MDS Manager software component

The MDS Manager software component provides all of the security functions expected for a secure network device as defined in the [NDcPP].

The TOE is a hardware appliance with embedded software installed at the factory. The TOE must be initially configured (e.g., network addresses, default routes, administrator accounts) using a command line interface from a local directly connected console.

Once network interfaces have been configured on an appliance, administration of the TOE is performed either from a local, directly connected console, or from a networked administrative workstation. Administration from a network workstations is performed using either an SSH protected terminal emulator or a TLS protected browser connection.

The AhnLab MDS products come packaged with MDS Agent software that can be subsequently installed on a host/PC to support the product’s malware detection and mitigation functions. When installed, the

Agent software does not execute within the MDS appliance and does not provide any of the TOEs security functions. In the evaluated configuration, the Agent software is not installed.

The following three figures show sample deployment topologies for each of the three TOEs. Note the product supports multiple deployments and as such shows some components or multiple TOEs in a deployment. In the evaluated configuration, distributed TOEs are not supported; each TOE instance is a single device. In addition, the evaluated configuration does not include agents for any of the TOE instances. Please see the AhnLab guidance documentation for more details on the other deployment options. To assist in interpreting the figures please refer to the following:

- Solid lines: physical networks
- Dotted lines: management communication: for example the Data Viewer in the MDS Manager device can manage agent status in Host Controller in MDS or MDS Manager devices
- Red dotted line: monitoring for traffic to MDS analyzer
- Green line: MDS agent deploy
- Triangle: mirrored port

Figure 1 depicts a sample topology for the MDS Appliance TOE.

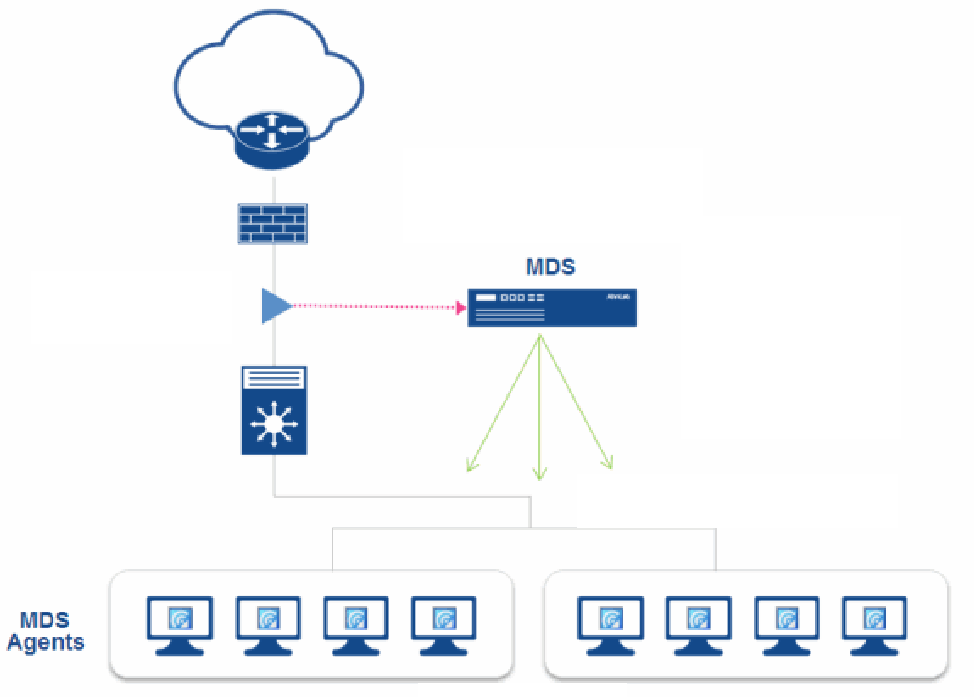

Figure 1: Sample MDS Network Topology

Figure 2 depicts a sample topology for the MDS Manager TOE. In the evaluated configuration, the MDS Manager TOE is installed as a single instance with both Data Viewer and Host Controller software and without an MDS Analyzer device. The figure depicts the MDS Managers deployed in two distinct roles – Data Viewer and Host Controller. The capabilities associated with each role are not covered by the evaluation, only the functions necessary to meet the requirements of [NDcPP].

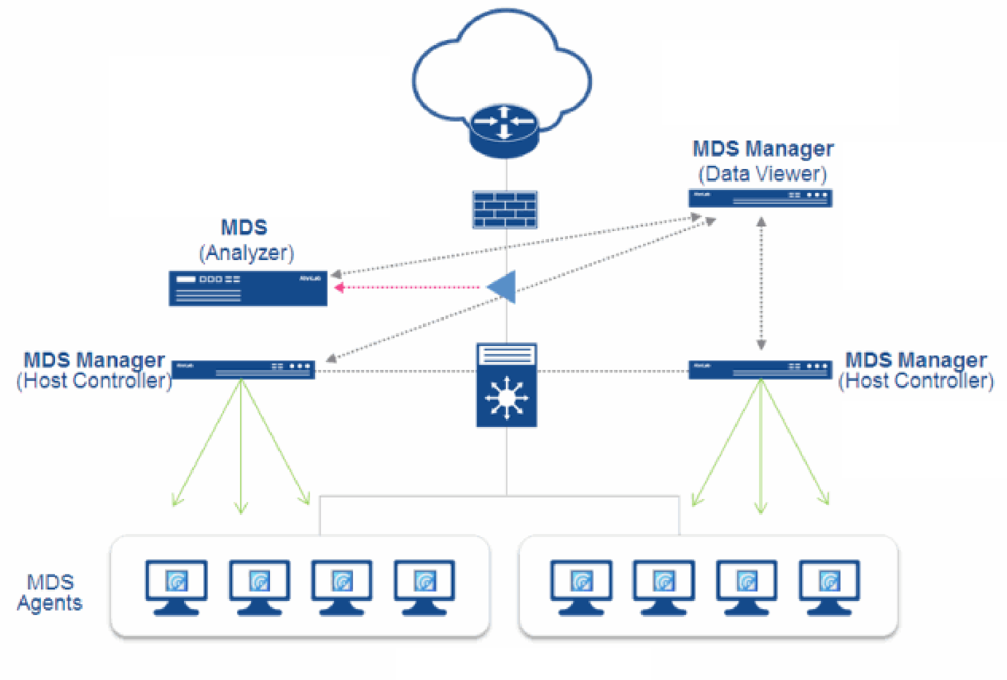

Figure 2: Sample MDS and MDS Manger Network Topology

Figure 3 depicts a sample topology for the MDS with MTA TOE.

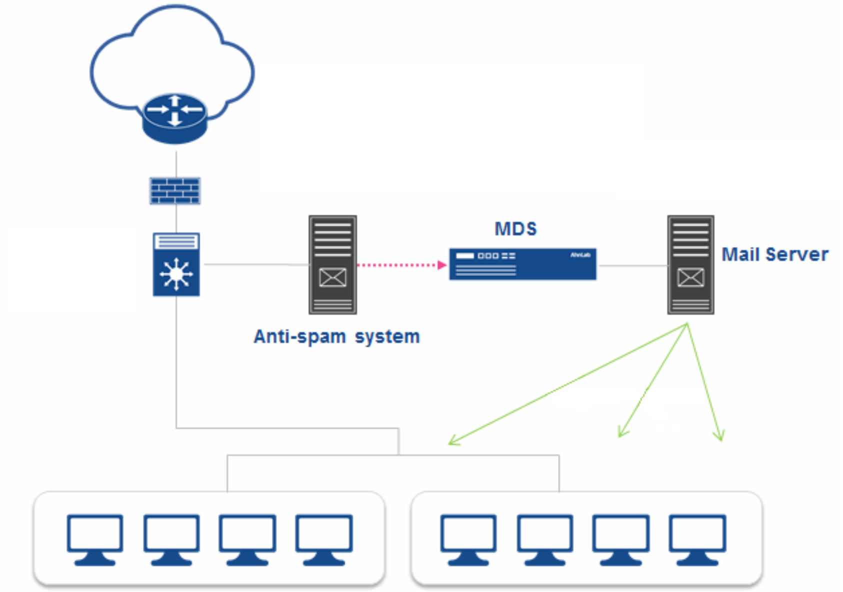

Figure 3: Sample MDS with MTA Network Topology

4 Assumptions

The Security Problem Definition, including the assumptions, may be found in the collaborative *Protection Profile for Network Devices* [NDcPP], version 1.0, February 27, 2015. That information has not been reproduced here and the NDcPP should be consulted if there is interest in that material.

5 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 PPs. 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.
5. The following specific product capabilities are excluded from use in the evaluated configuration:
    a. Non-FIPS 140-2 mode of operation—this mode of operation allows cryptographic operations that are not FIPS-approved
6. The TOE can be configured to rely on and utilize a number of other components in its operational environment:
    a. an external log server,
    b. an NTP server (optional), and
    c. An administrative workstation equipped with a Chrome version 40 (or higher) browser and SSH client software.

6 Security Policy

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

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

6.1 Security Audit

The TOE generates security relevant audit records including administrative activity. The audit records are stored on the TOE, protected from unauthorised deletion and can be sent to a remote audit server for storage. The connection for transmission of audit records uses TLS.

6.2 Cryptographic Support

The TOE includes cryptographic functionality that provide random bit-generation, encryption/decryption, digital signature, secure hashing and key-hashing features. These features support cryptographic protocols including SSH, TLS and HTTPS.

6.3 Identification and Authentication

The TOE identifies and authenticates all users prior to granting them access to the Web Management or Command Line interfaces. The TOE provides the ability to define administrative accounts that have permission to view and/or modify TOE configuration variables. Each of these administrative accounts has its own password.

The TOE provides Password Management restrictions including support for minimum characters, and restrictions for character usage.

The TOE provides X.509 Certificate Validation, Authentication, and X.509 Certificate Requests for certificates used in trusted channel protocols.

6.4 Security Management

The TOE offers two administrative interfaces a Command Line Interface (CLI) provided at a local console as well as through SSH and a graphical user interface provided through TLS/HTTPS. Both interfaces require a username and password prior to allowing any administrative actions to define accounts and configure TOE functionality. SSH also supports authentication via public-key. The System Administrator is considered to be the authorized Security Administrator of the TOE (as defined in the [NDcPP]). The TOE provides functions to manage the TOE and TOE data.

6.5 Protection of the TSF

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

The TOE ensures that sensitive information such as passwords and cryptographic keys are stored such that they are not accessible even to an administrator. The TOE provides its own internal clock which it uses to provide a reliable time source for audit records.

The TOE includes functions to perform self-tests and mechanisms for the update of the TOE software/firmware.

6.6 TOE Access

The TOE can be configured to display an informative banner when an administrator establishes an interactive session. The TOE can also enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated. Finally, the TOE allows administrators to terminate their own session.

6.7 Trusted Path/Channels

The TOE protects administrator communications from network workstations using SSHv2, TLS v1.1 and TLS v1.2 depending upon the interface being accessed. The administrative Command Line Interface is access through the SSHv2 protocol, while TLS/HTTPS is used for the Web Management interface. In each case, both integrity and disclosure protection is ensured by the protocol being used. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection is not established.

The TOE protects communication with an external log server to prevent unintended disclosure or modification of audit records.

7 Documentation

- AhnLab MDS V2.1, MDS Manager V2.1, MDS (MTA License Applied) V2.1 Configuring Common Criteria Compliance Guide

The following documents are available for additional guidance, but it is the supplement document above that serves to guide the user to operate the TOE in its evaluated configuration.

- AhnLab MDS Installation Guide, v1.1, 5/30/2016
- AhnLab MDS CLI Guide, v1.1, 5/30/2016
- AhnLab_MDS_Admin_Guide, v1.1, 5/30/2016
- AhnLab MDS (MTA) Installation Guide, v1.1, 5/30/2016
- AhnLab_MDS (MTA)_CLI Guide, v1.1, 5/30/2016
- AhnLab_MDS (MTA)_Admin Guide, v1.1, 5/30/2016
- AhnLab MDS Manager Installation Guide, v1.1, 5/30/2016
- AhnLab MDS Manager CLI Guide, v1.1, 5/30/2016
- AhnLab MDS Manager Admin Guide, v1.1, 5/30/2016

Supporting TOE Guidance Documentation

- AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Security Target, Version 0.3, April 26, 2017

8 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Common Criteria Test Report and Procedures Report Version 1.2, April 12, 2017

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the collaborative Protection Profile for Network Devices Version 1.0, 27 February 2015, [NDcPP] and including the following optional SFRs: FAU_STG.1, FCS_HTTPS_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.2, and FCS_TLSS_EXT.1.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the [NDcPP] Protection Profile. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the Leidos facility in Columbia, Maryland and concluded on April 12, 2017.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

8.1 Evaluated Configuration

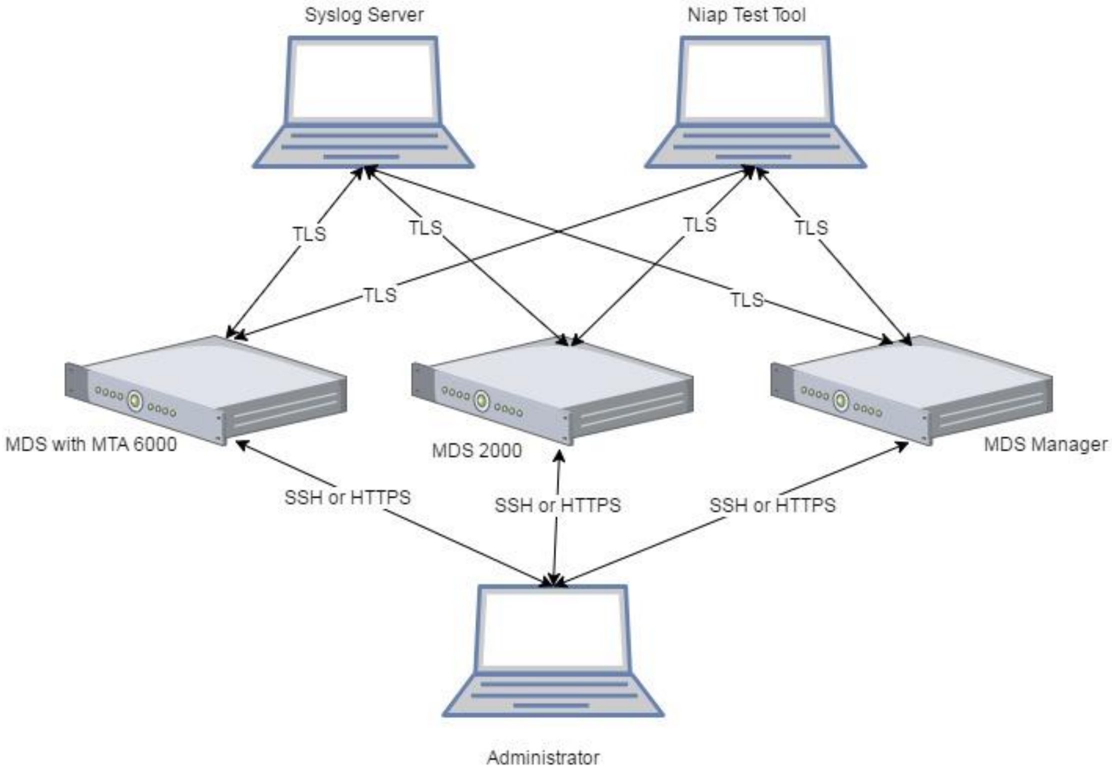

Figure 4 - Evaluated Configuration

8.2 Vulnerability Analysis

The evaluation team examined the CVEs applicable to the product in addition to the CVE-based hypotheses generated by the evaluators. The evaluation team also developed Types 3 and 4 flaw hypotheses in accordance with the [NDcPP] Section A.3, and that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the [NDcPP] Protection Profile; and the additional optional SFRs: FAU_STG.1, FCS_HTTPS_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.2, and FCS_TLSS_EXT.1, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 4 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

None

11 Annexes

Not applicable

12 Security Target

- AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Security Target, Version 0.3, April 26, 2017

13 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

Abbreviation	Description
AD	Active Directory
API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
GUI	Graphical User Interface
OS	Operating System
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMF	Service Management Facility
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Security Target, Version 0.3, April 26, 2017

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report For AhnLab MDS, MDS with MTA, and MDS Manager V2.1, Part 2 (Leidos Proprietary), Version 1.1, April 12, 2017