CSEC

Swedish Certification Body for IT Security

Certification Report - Forcepoint Triton APX 8.2

Issue: 1.0, 2017-jun-28

Authorisation: Imre Juhász, Lead Certifier , CSEC

Report Distribution:

Arkiv

Template: CSEC_mall_doc, 7.0

Table of Contents

1 Executive Summary 3

2 Identification 4

3 Security Policy 5

4 Assumptions and Clarification of Scope 7

4.1 Usage Assumptions 7
4.2 Environmental Assumptions 7
4.3 Clarification of Scope 7

5 Architectural Information 9

6 Documentation 11

7 IT Product Testing 12

8 Evaluated Configuration 14

9 Results of the Evaluation 15

10 Evaluator Comments and Recommendations 16

11 Glossary 17

12 Bibliography 18

Appendix A Scheme Versions 19

A.1 Scheme/Quality Management System 19

1 Executive Summary

The Target of Evaluation (TOE) is the TRITON APX 8.2 solution, including the Forcepoint V10000 G4 appliances on which the Forcepoint Web Security and Forcepoint Email Security components are installed. The TOE is a web proxy, residing between the internal and an external network, which it monitors in- and outbound network traffic applying filters and rules in order to protect the internal network and the resources residing there. The TOE is comprised of the following components:

- Forcepoint TRITON Manager 8.2.0.89
- Forcepoint Web Security 8.2.0.1264
- Forcepoint DLP 8.2.0.92
- Forcepoint Email Security 8.2.0.0101
- Forcepoint DLP Endpoint 8.2.0.2324 (Windows)
- Forcepoint DLP Endpoint 8.2.0.2323 (MacOS).

The evaluated deployment supports the TRITON APX components installed on On-Premise equipment.

The major security functionalities that the TOE offers are; security audit, user data protection, identification and authentication, security management, resource utilization and TOE access.

There are five assumptions made in the ST regarding the secure usage and environment of the TOE. The TOE rely on these being met in order to be able to counter the six threats in the ST. The assumptions and the threats are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by Combitech AB and EWA-Canada. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT security Evaluation, version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL2, augmented by ALC_FLR.2.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation. EWA-Canada operates as a Foreign location for Combitech AB within scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target, and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

- EAL2 + ALC_FLR.2.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.

This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2016010
Name and version of the certified IT product	TRITON APX 8.2 with Forcepoint Email Security and Forcepoint Web Security components running on Forcepoint V10000 Appliance Comprised of the following components: - Forcepoint TRITON Manager 8.2.0.89 - Forcepoint Web Security 8.2.0.1264 - Forcepoint DLP 8.2.0.92 - Forcepoint Email Security 8.2.0.0101 - Forcepoint DLP Endpoint 8.2.0.2324 (Windows) - Forcepoint DLP Endpoint 8.2.0.2323 (MacOS).
Security Target Identification	Security Target: TRITON APX 8.2 version 1.0
EAL	EAL2+ ALC_FLR.2
Sponsor	Forcepoint LLC
Developer	Forcepoint LLC
ITSEF	Combitech AB and EWA-Canada
Common Criteria version	3.1, revision 4
CEM version	3.1, revision 4
National and international interpretations	None
Recognition Scope	CCRA: EAL2+ALC_FLR.2, SOGIS-MRA: EAL2 and EA-MLA: EAL2+ALC_FLR.2
Certification date	2017-06-30

3 Security Policy

The TOE consists of seven security functions. Below is a short description of each of them. For more information, see Security Target [ST]

Security Audit

The TOE generates audit logs of Forcepoint TRITON Manager activity; recording administrator login attempts, policy changes, and configuration changes in the Audit Logs for each component. Only Super Administrators and System Administrators can review the audit logs. The TOE provides reliable timestamps to accurately record the sequence of events within the audit records.

User Data Protection

The TOE enforces web, data and email filters and policies on user traffic (inbound and/or outbound) to prevents internal entities from accessing potentially harmful or inappropriate content on external data, prevent loss of organization data and prevent infected email from entering the network.

Identification and Authentication

The TOE enforces identification and authentication for administrators before they can access any management functionality via the CLI. The TOE also prevents administrators from accessing Forcepoint TRITON Manager content before providing and authenticating a valid identity. The TOE maintains a list of security attributes (such as login credentials) for administrators. Depending on the web policy applied, unprivileged users are able to browse the internet anonymously. Email users have to identify and authenticate themselves before the TOE will permit access to their Personal Email Management UI to manage quarantined email messages.

Security Management

The TOE provides robust management interfaces that authorized administrators can use to manage the TOE and configure policies to control access to content. By default proxy filtering is enabled, but all traffic is allowed; therefore, the TOE has a permissive default posture. The TOE defines two categories of administrator — TRITON Administrator and Delegated Administrator.

Protection of the TSF

Communications to the Forcepoint DLP Endpoint client devices, from the Secondary Forcepoint DLP Server, are transmitted over HTTPS connections. The TOE protects these transmissions between the Secondary Forcepoint DLP server component and the Forcepoint DLP Endpoint client device from disclosure and modification by encrypting the transmissions under TLS v1.0.

Resource Utilization

The TOE enforces maximum limits on usage and availability of controlled traffic.

TOE Access

The TOE can assign a limit on the number of concurrent sessions that administrative users are allowed to have with Forcepoint TRITON Manager. If this limit is reached, the TOE prevents any new sessions from being created.

A TRITON console session ends 30 minutes after the last action taken in the user interface (clicking from page to page, entering information, caching changes, or saving changes). A warning message is displayed 5 minutes before session end.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The following assumptions about the usage are made:

A.INSTAL: TRITON-APX has been installed and configured according to the appropriate installation guides.

A.NOEVIL: It is assumed that administrators who manage TRITON-APX are not careless, negligent, or willfully hostile; are appropriately trained; and follow all guidance. Similarly is it assumed that users of the TRITON-APX endpoint component are not negligent or willfully hostile.

A.MANAGE: There are one or more competent individuals assigned to manage TRITON-APX and the security of the information it contains.

4.2 Environmental Assumptions

The following assumption about the environment are made:

A.NETWORK: All policy-controlled traffic between the internal and external networks traverses TRITON-APX.

A.LOCATE: It is assumed that the TRITON-APX appliance and associated servers are located within the same controlled-access facility and exclude unauthorized access to the internal physical network.

4.3 Clarification of Scope

The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation.

The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network.

The identified threats against the TOE are listed below:

T.EXTERNAL_CONTENT: A user on the internal network may access or post content to an external network that has been deemed inappropriate or potentially harmful to the internal network.

T.DATA_LOSS: A user may intentionally or inadvertently release sensitive data to unauthorized recipients.

T.MASQUERADE: A user may masquerade as another entity in order to gain unauthorized access to user data or TRITON-APX controlled resources.

T.NACCESS: An unauthorized person or external IT entity may be able to view or modify TRITON-APX configuration and control data by hijacking an unattended administrator session.

T.UNAUTHORIZED_ACCESS: A user may gain access to security data controlled by TRITON-APX that they are not authorized to access.

T.RESOURCE: TRITON-APX users or attackers may cause network connection resources to become overused and therefore unavailable

5 Architectural Information

The TOE physical boundary is shown in Figure 1.

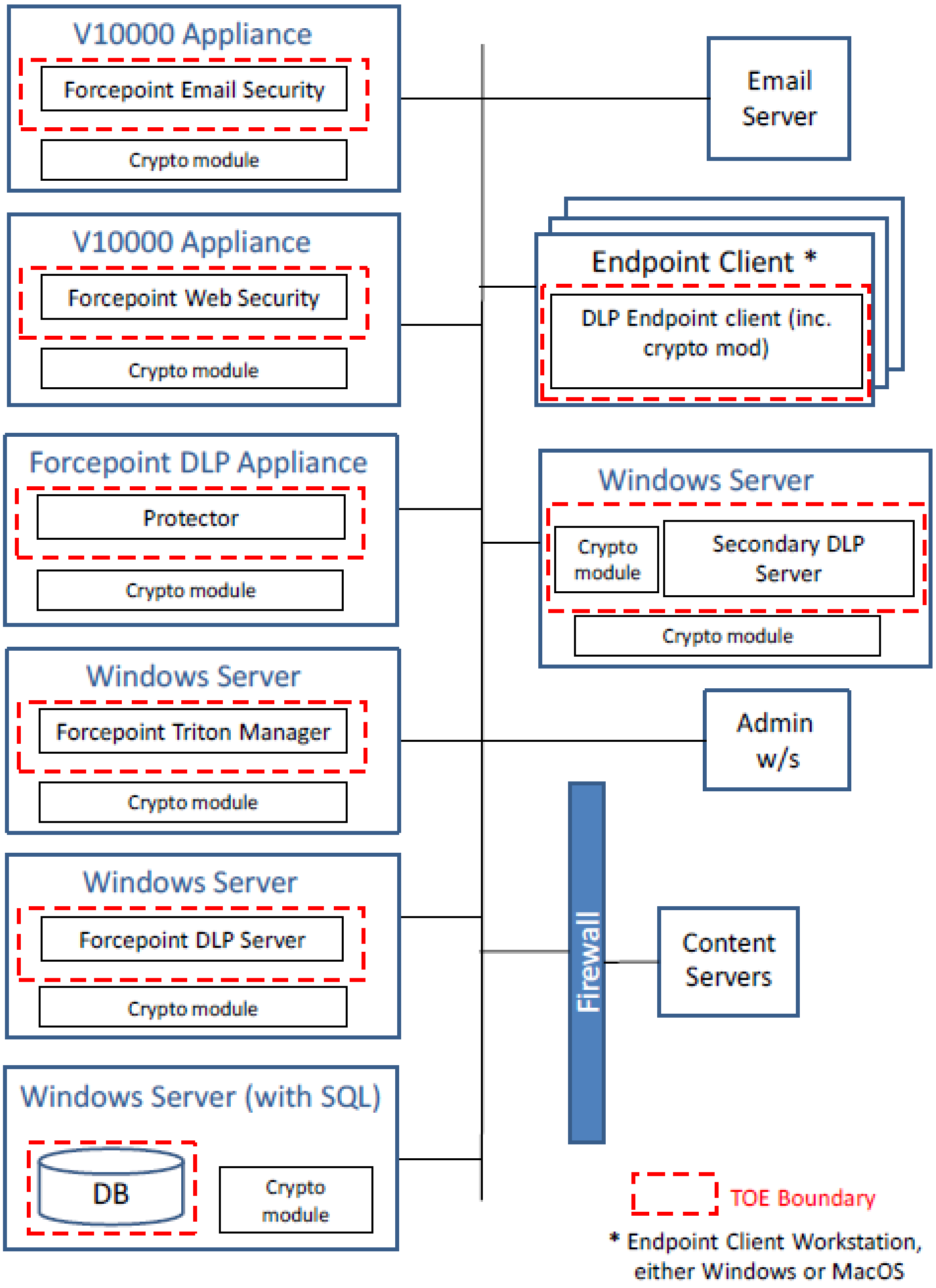

Figure 1, Physical TOE Boundry

5.1.1 The TOE is comprised of the following subsystems:

Core (CentOS Hypervisor) Subsystem

The Core Subsystem whose purpose is to provide the implementation of the TOE's physical hardware, including the Xen hypervisor, and hosted CentOS operating system.

Appliance Controller Subsystem

The Appliance Controller Subsystem provides administrators with access to setup and manage the appliance. The Appliance Controller Subsystem processes commands entered through one of the management interfaces to request updates to configuration changes as needed.

Content Gateway Subsystem

The Content Gateway Subsystem whose purpose is to enforce proxy filtering policies by delivering policy decisions to permit or deny access to requested Web content.

Network Agent Subsystem

The Network Agent monitors Internet traffic and filters non-HTTP protocols such as instant messaging. It provides bandwidth optimization data and enhanced logging detail.

Web Filtering Subsystem

The Web Filtering Subsystem whose purpose is to calculate proxy filtering policies by reading and interpreting policy rules.

Email Security Gateway Subsystem

Email Security Gateway filters email traffic by managing IP addresses and domain names. Traffic coming from certain IP address and domain names can be blocked or allowed through filtering rules defined by the administrator

6 Documentation

The physical scope of the TOE also includes the following guidance documentation:

- Installation Guide Forcepoint TRITON APX v8.2.x
- Installation Instructions TRITON AP-Web v8.2.x
- Installation Guide Forcepoint TRITON AP-Data Gateway and Discover v8.2.x
- Installing email protection appliance-based solutions, Email Protection Solutions, Version 8.2.x
- Installation and deployment guide Forcepoint Endpoint Solutions v8.2.x
- TRITON Manager Help Forcepoint TRITON Solutions v8.2.x
- Administrator Help Forcepoint TRITON AP-Web v8.2
- Administrator Help Forcepoint TRITON AP-Data Gateway and Discover v8.2
- Administrator Help Forcepoint TRITON AP-Email v8.2
- V-Series Appliance Manager Help TRITON AP-Web, TRITON AP-Email, Web Filter & Security, Models V10000, V5000. v8.2.x
- Content Gateway Manager Help Forcepoint Content Gateway, v8.2.x
- TRITON AP-Email Personal Email Manager User Help v8.2.x
- Quick Start Guide V10000 G22
- TRITON *APX 8.2Common Criteria Guidance Supplement*, *v1.0*

7 IT Product Testing

Both the developer and evaluator testing were executed at Forcepoint site in San Diego, USA.

Developer Tests

The general test approach was to provide a specific functional test for each behavioral implication of the Security Functional Requirements claimed in the Security Target. The tests focused on covering all security behaviors and ensuring that the functional testing was thorough without being unnecessarily detailed.

Test Runs were functional tests conducted externally and manually. Test Procedures involve actions taken by the tester through the following external interfaces:

- Appliance Controller GUI
- Appliance Controller CLI
- Content Gateway GUI
- TRITON Manager GUI
- Authentication Interface
- Content Gateway Traffic Interface
- Email Security Gateway Traffic Interface
- Network Agent Traffic Interface
- Data crawler

The functionality of the product was tested through usage scenarios. The basic functionality of the TOE was tested when the tester initially set up the TOE by following the procedures outlined in the installation and setup documentation.

Independent Evaluator Tests

The evaluator conducted nineteen different test cases divided into four different test groups:

- Test Group 1: TOE Installation, verification of the guidance documentation
  - Test Case 1.1 – Walkthrough of TOE installation
- Test Group 2: Repetition of a chosen subset of developer tests
  - Re-test of a subset of the developer tests
- Test Group 3: Additional tests defined by the evaluator
  - Delay caused by incorrect login
  - User Data Protection (email quarantine, virus)
  - TOE implementation of FMT_SMF.1
- Test Group 4: Penetration testing (vulnerability scanning)
  - Vulnerability scanning, TRITON Manager
  - Vulnerability scanning, Forcepoint DLP Secondary Server

The results of all the test cases were consistent with the expected test results and all tests were judged as pass.

Penetration Tests

Vulnerability and port scanning were performed using Nessus vulnerability scanner at Forcepoint Triton Manager and Forcepoint DLP Secondary Server, Endpoint interface. No high severity vulnerabilities were found. The Medium severity findings were analyzed and none of the vulnerabilities were found exploitable in TOE operational environment.

An additional analysis was performed since the endpoint client is outside of the controlled environment and therefore is more exposed to attackers. That an attacker is to carry out any potent attack against the TOE is judged low since:

- This data flow is protected by TLS
- The traffic between an endpoint client and the secondary DLP server is not thought of as being sensitive.
- Due to Perfect Forward Secrecy an attacker would have to extract every session key to decrypt every session to have a continuous flow of information.

8 Evaluated Configuration

The server components of the TOE are intended to be deployed in a physically-secured cabinet room, room, or data center with the appropriate level of physical access control and physical protection (e.g. fire control, locks, alarms, etc.). Access to the physical console or USB ports on the appliance and associated TOE servers should be restricted via a locked data cabinet within the data center. The TOE is intended to be managed by administrators operating under a consistent security policy. In addition, any authentication server used by the TOE (e.g. Active Directory server) should also be hosted within this secured environment. The TOE environment is responsible for providing protection of network communication between the TOE server components and also between the TOE and the administrative user.

Dependencies to Other Hardware, Firmware and Software

The TRITON Manager, Web Log Server and Email Log are not hosted on the Forcepoint appliance. These TOE components are installed on Microsoft Windows server (these components are installed on a single server in the evaluated deployment). The TRITON solution also requires a Microsoft SQL Server to host the Log Server Database (the Database and Forcepoint TRITON Manager must be hosted on separate servers). In the evaluated deployment these components are all installed on Windows Servers.

The ST specifies the minimum requirements regarding the hardware needed in the enviroment. The following minimum platform requirements specified in the ST are necessary for the deployment of the Forcepoint DLP Endpoint component, depending on the type of endpoint device. The platforms may either be physical devices or provided by Citrix XenDesktop v7.6:

- Forcepoint Triton Manager
- Microsoft SQL Server
- Forcepoint DLP (data security) Servers (primary and secondary)
- Forcepoint DLP Appliance (Protector)
- Windows Forcepoint DLP Endpoint Client
- MacOS Forcepoint DLP Endpoint Client

The Forcepoint TRITON Manager is accessed via a web browser on a management workstation using a standard web browser (such as Internet Explorer 11, Firefox 40).

Excluded from the TOE Evaluated Configuration

Features/Functionality/Components that are not part of the evaluated configuration of the TOE are:

- Hybrid Services (Web Hybrid Module and the Email Hybrid Module).
- Optional Web components, including Remote Filtering Server, Sync Service, and transparent identification agents (DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent).
- Forcepoint DLP Endpoint DLP used in Forcepoint DLP hybrid and cloud deployments.
- Forcepoint DLP ENDPOINT Web and Remote Filtering clients.

9 Results of the Evaluation

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name	Verdict
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security objectives	ASE_OBJ.2	PASS
Extended components definition	ASE_ECD.1	PASS
Derived security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Life-cycle support	ALC	PASS
Use of a CM system	ALC_CMC.2	PASS
Parts of the TOE CM Coverage	ALC_CMS.2	PASS
Delivery procedures	ALC_DEL.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Development	ADV	PASS
Security Architecure description	ADV_ARC.1	PASS
Security-enforcing functional specification	ADV_FSP.2	PASS
Basic design	ADV_TDS.1	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Tests	ATE	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - Sampling	ATE_IND.2	PASS
Vulnerability assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

The evaluator has no recommendation for the TOE.

11 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
CentOS	Community Enterprise Operating System
CLI	Command Line Interface
DLP	Data Loss Prevention
EAL	Evaluation Assurance Level
HTTPS	Hypertext Transfer Protocol (Secure)
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
GUI	Graphical User Interface
LAN	Local Area Network
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

12 Bibliography

[CCp1]	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 4, September 2012, CCMB-2012-09-001
[CCp2]	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 4, September 2012, CCMB-2012-09-002
[CCp3]	Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 4, September 2012, CCMB-2012-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012, CCMB-2012-09-004
[ST]	Forcepoint, Security Target, TRITON APX 8.2 , Forcepoint LLC., 2017-04-27, version 0.11

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
1.20.4	2017-05-11	*None*
1.20.3	2017-04-24	*None*
1.20.2	2017-02-27	*None*
1.20.1	2017-01-12	*None*
1.20	2016-10-20	*Original version*

Scheme Notes Release 9.0:

- Scheme Note 15 - Demonstration of test coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target