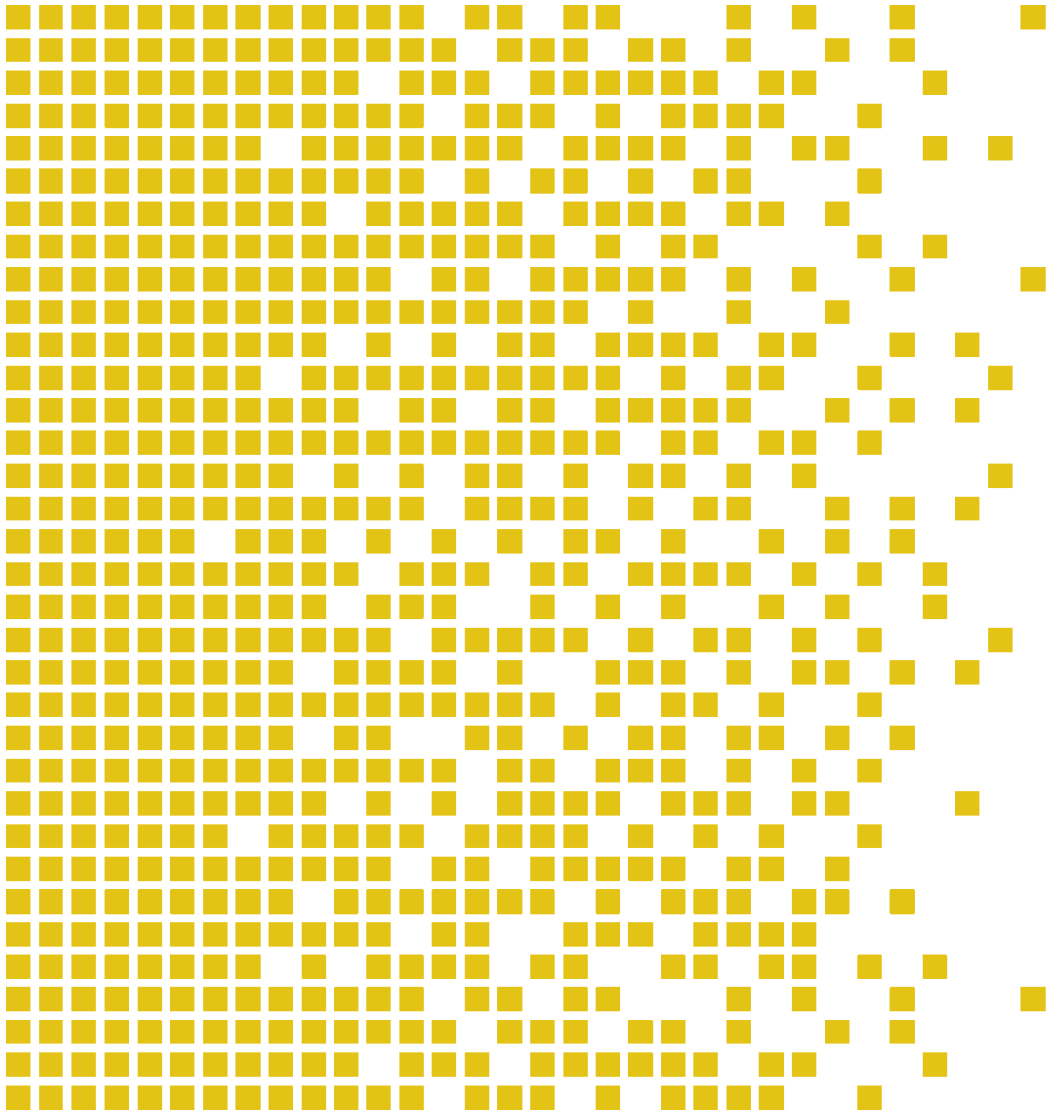
SERTIT-046 CR Certification Report

Issue 1.0 12 February 2013

The AX Series Advanced Traffic Manager, AX3200-12, AX1030, AX5630, AX3530



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

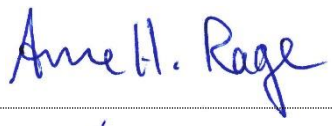
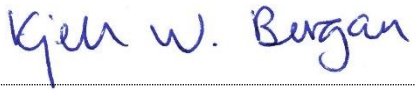
The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Contents

1 Certification Statement

The A10 Networks' The AX Series Advanced Traffic Manager is a series of traffic managers designed to help enterprises and ISPs with application availability through a Web Application Delivery Platform. The TOE are hardware devices with the same security functionality, but with different performance parameters.

The AX Series Advanced Traffic Manager versions AX3200-12, AX1030, AX5630, AX3530 with software version 2.7.0-P1 have been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.1for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality (see Security Target chapter 5) when running on the platforms specified in Annex A.

Author	Rage, Arne Høye Certifier	
Quality Assurance	Lars Borgos Quality Assurance	
Approved	Kjell W. Bergan Head of SERTIT	
Date approved	12 February 2013	

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CMVP	Cryptographic Module Validation Program
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
FIPS	Federal Information Processing Standard
HMAC	Hash-based message authentication code
HTTPS	Hypertext Transfer Protocol Secure
ISP	Internet Service Provider
SERTIT	Norwegian Certification Authority for IT Security
SFP	Security Function Policy
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF/TSFI	TOE Security Function/TOE Security Function Interface

3 References

[1] Security Target for A10 Networks Advanced Traffic Manager AX3200-12, AX1030, AX5630, AND AX3530 (Applications Delivery Controller), v.1.4, February 08, 2013.

[2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[7] Evaluation Technical Report for the evaluation project SERTIT-046, A-A10-2-ATM-ETR-1.1, February 08, 2013.

(For references to guidance documents, see Annex A.)

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of The AX Series Advanced Traffic Manager version AX3200-12, AX1030, AX5630, AX3530 to the developer A10 Networks, Inc., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The versions of the product evaluated were The AX Series Advanced Traffic Manager and versions AX3200-12, AX1030, AX5630, AX3530 with software version 2.7.0-P1

These products are also described in this report as the Target of Evaluation (TOE). The developer was A10 Networks, Inc.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The scope of the evaluation includes software and hardware that form the TOE and the TOE security functions that are stated in the Section 7.1 in the Security Target[1] For The AX Series Advanced Traffic Manager

- High Availability feature is outside of the scope of the evaluation.
- The Data Plane of AX Series Advanced Traffic Manager shall not have open ports that are serviced by AX Series Advanced Traffic Manager (such as ssh management, etc.)
- There is no IP routing between the Management Plane and the Data Plane, therefore AX Data plane users cannot access the management plane.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL 2 augmented with ALC_FLR.1 was used. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

P.Cryptography: The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.

P.Cryptography_Validated: Only FIPS 140-1/2 validated cryptography (methods and implementations) are acceptable for key management (i.e., generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

P.Manage: The TOE shall only be managed by authorized users.

P.Access: All data collected and produced by the TOE shall only be used for authorized purposes.

P.Integrity: Data collected and produced by the TOE shall be protected from modification.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats, OSP's and assumptions which these objectives meet and security functional requirements and security functions to elaborate the objectives. The SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products. There are however some functional components that are extended. The rationale for these components can be found in the Security Target[1], chapter 5.

4.8 Threats Countered

TT.Masquerade: A hacker may masquerade as another entity in order to gain unauthorized access to data or TOE resources.

TT.Tampering: A hacker may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.

TT.Access_TOE: A user may gain unauthorized access to security data on the TOE due to SLB failure.

TT.Access_Int: A user may gain unauthorized access to server resources on protected/internal network.

TT.Mod_Conf: A hacker may modify the TOE configuration to gain unauthorized access to server resources on protected/internal network.

4.9 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.10 Environmental Assumptions and Dependencies

A.Install: The TOE has been installed and configured according to the appropriate installation guides, and all traffic between clients and servers flows through it.

A.Manage: There is one or more competent individual (administrator) assigned to manage the TOE and the security of the information it contains.

A.No_Evil: The administrators of the TOE are non-hostile, appropriately trained, and follow all guidance.

A.Locate: The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4.11 IT Security Objectives

O.Load_Balancing: The TOE must provide encrypted SSL connections for load balanced servers with basic firewall protection.

O.Cryptography: The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE.

O.Cryptography_Validated: The TOE will use CMVP FIPS 140-1/2 validated crypto modules for cryptographic services implementing CMVP -approved security functions and random number generation services used by cryptographic functions.

O.Protect: The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data, and preserve correct operations during specified failure events.

O.Admin: The TOE must include a set of functions that allow management of its functions and data, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators, may exercise such control.

O.Authenticate: The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.

O.Audit: The TOE must record the actions taken by administrators, prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.

O.Time: The TOE must provide reliable timestamps for its own use.

O.Access_Int: The TOE must allow access to server resources on protected/internal network only as defined by the Information Flow Control SFP.

O.Integrity: The TOE must ensure the integrity of all audit and system data.

4.12 Non-IT Security Objectives

OE.External: The TOE environment must ensure any authentication data in the environment are protected and maintained.

OE.Manage: Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the

TOE's timestamps will be ensured via periodic manual checks by the TOE administrator.

OE.Connect: The TOE environment must provide network connectivity to the TOE. The network connection to the TOE must be reliable.

OE.Power: The TOE environment must provide the electricity necessary to the TOE to function. The power to the TOE must be reliable and protected from surges and disconnects.

OE.AC: The TOE environment must regulate the temperature of the facility where the TOE is located so no damage is caused by heat or cold.

OE.Physical: The physical environment must be suitable for supporting a computing device in a secure setting.

OE.Install: Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

OE.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.

4.13 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

- FLB_SCO_EXP.1 Secure communication
- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SAR.1 Audit review
- FAU_SAR.3 Selectable audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.4 Prevention of audit data loss
- FCS_BCM_EXP.1 Baseline cryptographic module
- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.2 Cryptographic key distribution
- FCS_CKM.4 Cryptographic key destruction
- FCS_COP_EXP.1 Random Number Generation
- FCS_COP_EXP.2 Cryptographic Operation
- FDP_ACC.1a Subset access control – Administrator Access Control
- FDP_ACC.1b Subset access control – SSL Access Control
- FDP_ACF.1a Security attribute based access control - Administrator Access Control
- FDP_ACF.1b Security attribute based access control - SSL Access Control
- FDP_IFC.1 Subset information flow control
- FDP_IFF.1 Simple security attributes
- FIA_ATD.1 User attribute definition
- FIA_UAU.1a Timing of authentication - Administrator
- FIA_UAU_EXP.1 Timing of authentication – User
- FIA_UAU.5 Multiple authentication mechanisms
- FIA_UID.1 Timing of identification

- FMT_MOF.1 Management of security functions behaviour
- FMT_MSA.1 Management of security attributes
- FMT_MSA.2 Secure security attributes
- FMT_MSA.3a Static attribute initialisation - Administrator Access Control SFP
- FMT_MSA.3b Static attribute initialisation - SSL Access Control SFP
- FMT_MSA.3c Static attribute initialisation – Information Flow Control SFP
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FPT_FLS.1 Fail secure
- FPT_ITC.1 Inter-TSF confidentiality during transmission
- FPT_ITT.1 Basic internal TSF data transfer protection
- FPT_STM.1 Reliable time stamps

4.14 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by Advanced Data Security (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT 08 February 2013. SERTIT then produced this Certification Report.

4.15 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is

not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

The developer ships products using shipping boxes with sealed tape.

A cryptographic signature is used to verify the integrity of the software upon receipt (or first use) of the product. HMAC signature is used to satisfy the FIPS 140-2 requirement. Tamper proof seals are used to secure the product.

HTTPS cryptographic signatures are used to verify the integrity of the software upon electronic transfer of software.

The access to the software downloads is controlled, and the corresponding mechanism uses user name and password. Users registered to Support Web Portal and selected user id and password.

The software downloads are encrypted by an HTTPS session. Self-Signed Certificate is used for software distribution

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with all the documents that comprise the administrator guidance, user guidance and installation guide provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Users of the TOE should follow the guidance for the TOE in order to ensure that it operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process. The evaluators have searched for potential vulnerabilities and penetration tests have been devised and performed. The evaluators have not found any exploitable vulnerabilities or residual vulnerabilities in the TOE.

5.6 Developer's Tests

The evaluators have examined the developers test plan and determined that it describes the scenarios for performing each test, including any ordering dependencies on results of other tests. The test plan provides information about the test configuration being used: both on the configuration of the TOE and on any test equipment being used, as well as information about how to execute the tests.

All TSFIs are covered by the developer's tests.

5.7 Evaluators' Tests

The evaluators have employed a combination of a random sampling method and a method based on their intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible. The testing covered the following:

1. The use of the access control lists.
2. Load balancing using network protocols.
3. Tests of system functions.
4. Testing of encrypted user traffic.
5. Testing of secure administrative sessions via SSH and HTTPS.
6. Testing of logging.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the evaluators, and the conduct of the evaluation, as witnessed by the certifier, SERTIT has determined that The AX Series Advanced Traffic Manager versions AX3200-12, AX1030, AX5630, AX3530 meets the Common Criteria Part 3 conformant requirements Evaluation Assurance Level EAL 2 augmented with ALC_FLR.1 extended functionality in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of The AX Series Advanced Traffic Manager versions AX3200-12, AX1030, AX5630, AX3530 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 "TOE Scope" and Section 5 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

The above "Evaluation Findings" include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Advanced Traffic Manager AX3200-12, AX1030, AX5630, AX3530.

Hardware versions: AX3200-12, AX1030, AX5630, AX3530.

Software version: 2.7.0-P1

TOE Documentation

The supporting guidance documents evaluated were:

[a] Security Target for A10 Networks Advanced Traffic Manager AX3200-12, AX1030, AX5630, and AX3530 (Applications Delivery Controller). Version 1.4

[b] FIPS 140-2 Level 2 Security Policy For AX Series Advanced Traffic Manager AX2500, AX2600-GCF, AX3000-GCF, AX5100 and AX5200, Version 0.3

[c] System Configuration and Administration Guide, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0024, Ver. 2.7.0 11/2/2012

[d] aFleX Scripting Language Reference, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0007, aFleX Engine Ver. 2.0 5/4/2011

[e] aXAPI Reference, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0010, Ver. 2.6, 5/4/2011

[f] Command Line Interface Reference, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0003, Ver. 2.6.1 5/6/2011

[g] Graphical User Interface Reference, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0002, Ver. 2.6.1 5/6/2011

[h] Management Information Base Reference, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0008, Ver. 2.6.1 5/4/2011

[i] Application Delivery and Server Load Balancing Guide, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0026, Ver. 2.6.1-GR1 4/18/2012

[j] Global Server Load Balancing Guide, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0029, Ver. 2.6.1-GR1 4/17/2012

[k] Installation Guide for the AX 1000 / AX 1000-11, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0011, 5/4/2011,

[l] Installation Guide for AX 2000, AX 2100, AX 2200, AX 2200-11, AX 3100, AX 3200, and AX 3200-11, AX Series Advanced Traffic Manager, Document No.: D-030-02-00-0009, 5/4/2011

[m] Installation Guide for AX 2500, AX 2600, AX 3000, AX 3000-11, and AX 3000-11-GCF, AX Series Advanced Traffic Manager, Document No.: D-030-02-00-0014, 5/4/2011

[n] Installation Guide for AX 5100 and AX 5200, AX Series Advanced Traffic Manager, Document No.: D-030-02-00-0015, 5/4/2011

[o] Installation Guide for AX 1030 / AX 3030, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0031, 11/2/2011

[p] Installation Guide for AX 2500, AX 2600, AX 3000, AX 3000-11, AX 3000-11-GCF, AX 3200-12, and AX 3400, AX Series Advanced Traffic Manager, Document No.: D-030-02-00-0014, 2/13/2012

[q] Installation Guide for AX 3530, AX Series Advanced Traffic Manager, Document No.: D-030-01-00-0038, 7/3/2012

[r] Installation Guide for AX 5630, AX Series Advanced Traffic Manager, Document No.: D-030-02-00-0046 11/2/2012

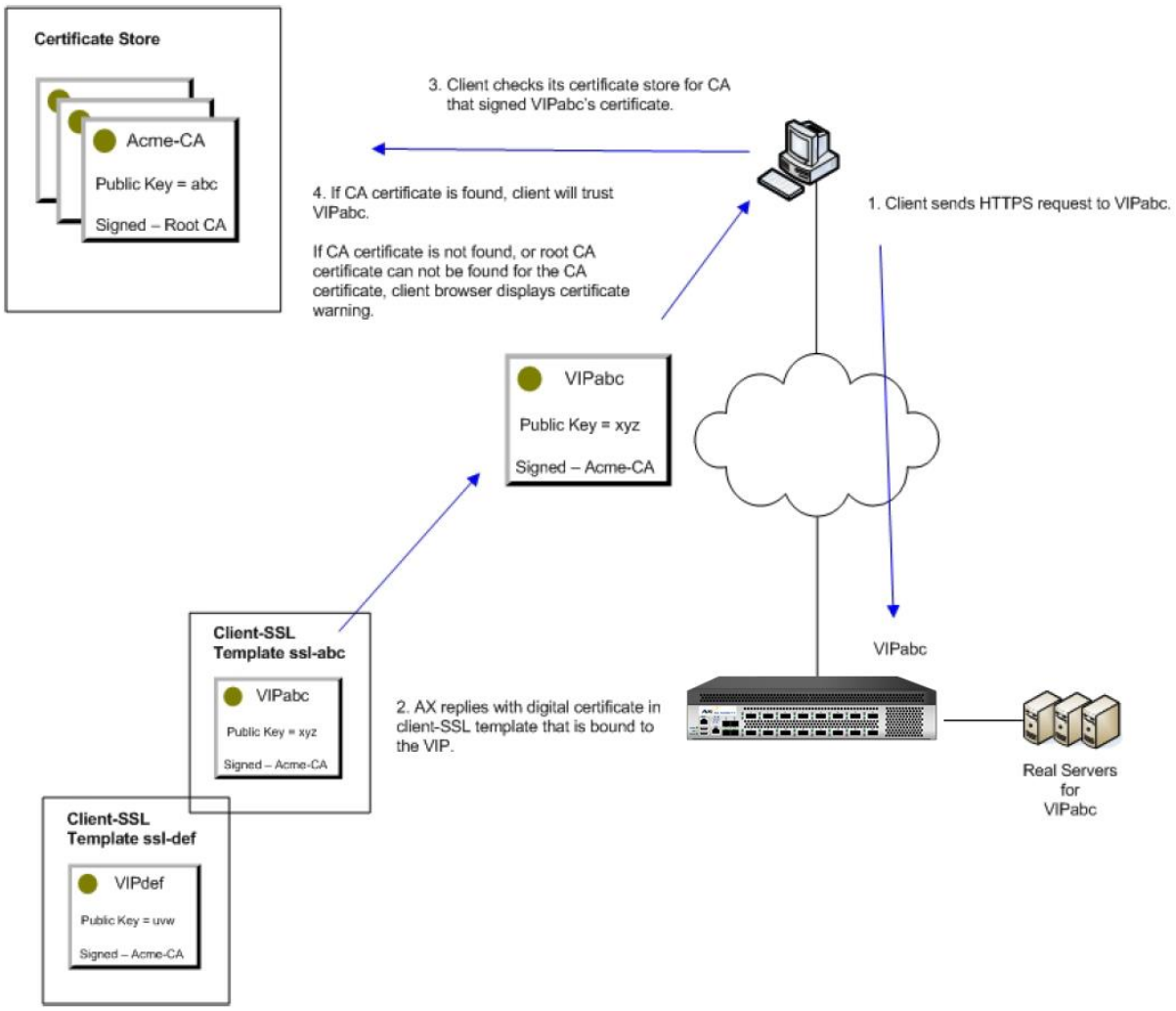
[s] Release Notes, AX Series Advanced Traffic Manager, Document No.: D-030-02-00-0001

[t] SoftAX Installation Guide, AX Series Advanced Traffic Manager, Document No.: D-030-02-00-0016 5/4/2011

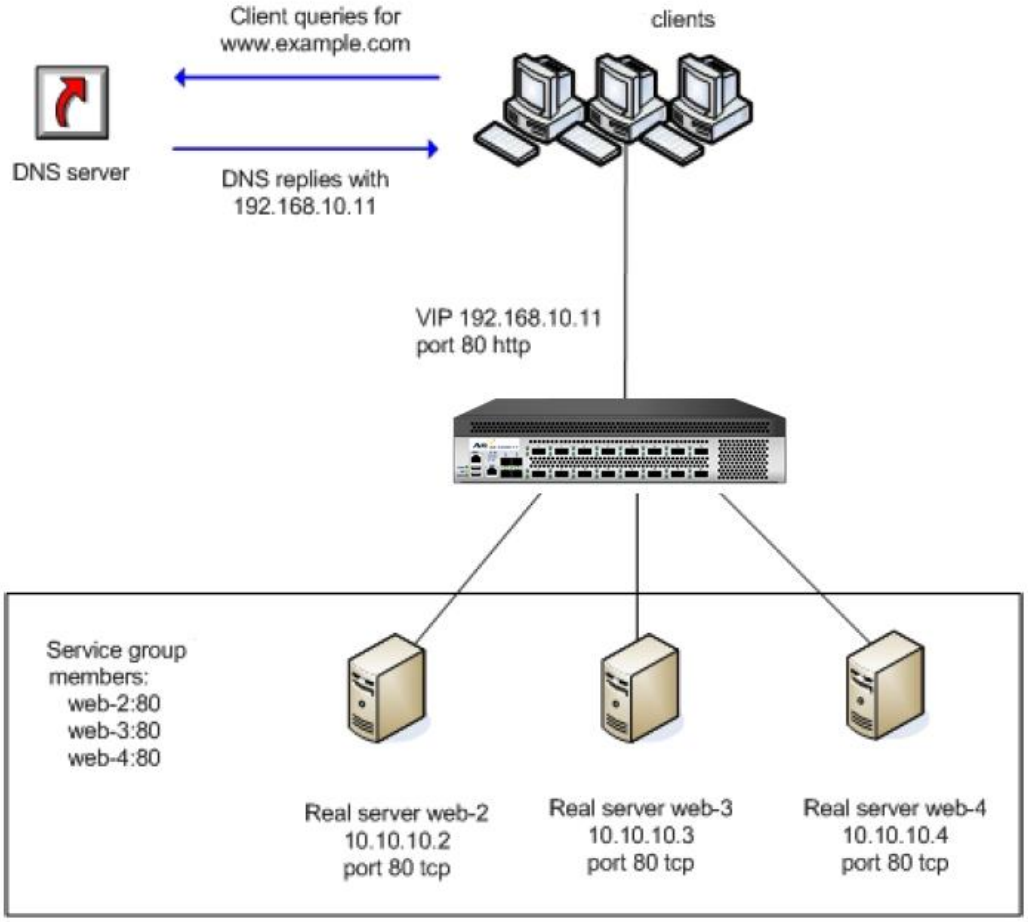
TOE Configuration

The following configuration was used for testing:

Secure client-server traffic:



Server load balancing:



The following tools were used during the evaluation

- Nessus Vulnerability Scanner, Version 5.0.1
- Nmap Security Scanner, Version 6.01
- Wireshark Network Protocol Analyzer - version 1.8.1
- OpenSSH Client, Version 5.8
- PuTTY - release 0.62

Evaluated configuration included the following:

- TOE A10 Networks Advanced Traffic Manager configured to run in the Common Criteria evaluated configuration that is specified in the guidance documentation. More specifically:
  - The High Availability feature was not enabled

- The Data Plane of Advanced Traffic Manager did not have open ports that were serviced by Advanced Traffic Manager (such as ssh management, etc.)
- There was no IP routing between the Management Plane and the Data Plane, therefore AX Data plane users could not access the management plane.

Environmental Configuration

The TOE is stand alone boxes consisting of hardware and software.