IPSEC Basic Certification Testing Report
Version 3.1

A10 Networks
A10 Networks Thunder Series

March 22, 2022

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

Table of Contents

A10 Networks - A10 Networks Thunder Series
IPSEC Basic Certification Testing Report

Executive Summary

Introduction

The goal of ICSA Labs certification testing is to significantly increase user and enterprise trust in information security products and solutions. For more than 30 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

Product Overview

The A10 Networks Thunder Series from A10 Networks delivers high performance application networking and security solutions. The A10 Networks Thunder Series allows for the integration and expansion of system resources to support future feature needs, while offering A10 Networks broadest array of physical, virtual and hybrid form factors.

Scope of Assessment

The ICSA Labs IPSEC Product Certification Program has the objective to make available to the end user community an ever-increasing selection of IPSEC products that are interoperable and that provide the security services of authentication, data integrity, and confidentiality. The IPSEC Product Certification Criteria, Version 3.1 is based on the Internet Key Exchange version 2 (IKEv2), and IPSEC protocols. ICSA Labs tested the product against its "BASIC" requirements. The set of requirements are summarized below.

The following is a summary of the IPSEC 3.1 BASIC requirements against which the product was tested:

- The IPSEC Product must be a generally available product and must be interoperable (negotiation, establishment, and rekeying of SAs) with other independent implementations.
- The IPSEC Product must be in compliance with a specific subset of requirements defined in the IETF IPSEC related RFCs.
- The IPSEC Product must be in compliance with a specific subset of requirements defined in the IETF IKEv2 related RFCs.
- The IPSEC Product must implement cryptographic algorithms without fatal or security-degrading mistakes.
- The IPSEC Product must not be vulnerable to an evolving set of remotely executable exploits related to the IKEv2/IPSEC implementation that is known to the Internet community.
- The IPSEC Product must have the ability to log the required data for IKEv2 negotiation failures and other administrative changes.
- The IPSEC Product must provide cryptographically-protected remote administration.

Summary of Findings

With the successful testing of the TH-1040S model, both the tested model and the other members of the A10 Networks Thunder Series satisfied all of the mandatory certification testing requirements to retain ICSA Labs IPSEC Version 3.1 IKEv2 BASIC Certification.

Certification Maintenance

The IPSEC Product will remain certified on this and future released versions of the product for the length of the testing contract. Future versions continue to be certified since the product is continuously deployed at ICSA Labs and may be subjected to periodic testing on the most current product version.

Three circumstances will cause the IPSEC Product to have its certification revoked:

1. The IPSEC Product vendor withdraws from the ICSA Labs IPSEC Certification Program.
2. The product fails periodic testing and the IPSEC Product vendor subsequently fails to provide an adequate fix within a prescribed length of time.
3. The product fails to meet the next full test cycle against the current version of the criteria.

Product Description

The term IPSEC Product refers to the complete system submitted by the vendor for certification testing including all documentation, hardware, firmware, software, operating systems, and management systems. Common network services such as Syslog, DNS, NTP, etc. are provided by ICSA Labs and are not considered part of the IPSEC Product, unless otherwise noted.

Hardware

A10 Networks provided the following product for testing:

- **TH-1040S**

Software

Testing was successfully completed with version 5.2.1-P3 build 70.

Product Family Description

This section lists the members of the certified product family. A representative set of models was submitted for testing and listed in the Hardware section above. In order to submit a family of products for certification, the vendor must attest that:

- The vendor designs and maintains control over the entire set of hardware, firmware, and software for each member of the product family.
- The vendor software, including but not limited to the functional software and the operating system software, is uniform across the product family.
- The management interface(s) for the members of the product family are uniform and completely consistent.
- Each member in the product family has an equivalent set of functionality (in terms of security).
- The functional, integration, and regression testing conducted by the vendor is uniform and consistent across the product family.

Product Family Members

At the time of report writing, the models belonging to the A10 Network Thunder Series that are ICSA Labs IPSEC Version 3.1 Basic Certified include the following:

- TH-940
- TH-1040
- TH-3040
- TH-3350-E
- TH-3350
- TH-3350S
- TH-4435
- TH-4440
- TH-5440
- TH-5840
- TH-5840-11
- TH-5845
- TH-6440
- TH-7440
- TH-7440-11
- TH-7445
- TH-7650
- TH-7655
- TH-7655S
- TH-14045
- TH-ADC-for-Baremetal
- vThunder

Test Configuration

ICSA Labs installed and configured the IPSEC Product according to the vendor supplied documentation. Any special configurations or deviations from the vendor supplied documentation that were necessary to execute a test or meet a requirement are documented in this section.

The following is a list of parameters that were the basis for the initial IKEv2 tests.

IKEv2 SA parameters:

- AES-CBC-256 encryption
- HMAC-SHA-2 authentication/integrity
- DH Group 14 key exchange
- Preshared Key authentication

Child SA parameters:

- ESP tunnel mode
- AES-256 encryption
- HMAC-SHA-2 authentication/integrity

Configuration Notes

ICSA Labs performed the initial IPsec VPN configuration following the steps provided in the following guidance information, *Configuring IPsec VPN,* from A10 Networks.

- After configuring the IPsec VPN, the administrator must add a static route of type Tunnel with the Interface Number and the appropriate Next Hop IP based on the IPsec tunnel configuration.
- Narrowed Traffic Selectors can be specified in the IPsec tunnel configuration. Additionally, a related Firewall Ruleset must be configured to enfore the desired policy.

Detailed Findings

IKEv2/IPSEC Interoperability

The IPSEC Product was configured to establish IKEv2 and IPSEC Security Associations (SAs) with the peers in the table below. SAs were maintained following numerous successful rekey operations with traffic flowing in each direction.

Interoperability was tested successfully with the open source implementation of strongSwan (strongswan.org) and the following ICSA Labs certified IPSEC VPN products:

Vendor	Product Name	Product Version
F5 Networks	BIG-IP i10800	16.1.0 Build 0.0.19
Fortinet	FortiGate 101F	6.4.5 Build 5651

Cryptography

ICSA Labs verified the following algorithms, all of which are supported by the Candidate IPSEC Product:

- AES-CBC-256
- SHA2-256 authentication/integrity
- DH Group 14 key exchange

Administration

ICSA Labs verified that secure remote access was supported. Administration was performed using a web browser via HTTPS access. The use of SSH to access the ACOS command line interface (CLI) was also verified. In both cases, ICSA Labs confirmed the use of strong ciphers by the product under test.

Logging

ICSA Labs verified the required log data was captured for logging IKE negotiation failures and administrative events.

ICSA Labs analysts viewed detailed log entries using the CLI via ssh access. Log entries can viewed by entering the following commands after accessing the CLI and entering Enable mode:

```
#  debug vpn level 1
#  show vpn log follow
```

Below is an example of how the TH-1040S logs an IKE failure due to an mismatched pre-shared key settings:

```
Mar 15 03:22:14 87[IKE] <icsa_ike|15> initiating IKE_SA icsa_ike[15] to 1.1.4.1
Mar 15 03:22:14 87[ENC] <icsa_ike|15> generating IKE_SA_INIT request 0 [ SA KE No
N(NATD_S_IP) N(NATD_D_IP) ]
Mar 15 03:22:14 87[IKE] <icsa_ike|15> 205.160.10.1[500]->1.1.4.1[500]: [ SA KE No
N(NATD_S_IP) N(NATD_D_IP) ]
Mar 15 03:22:14 87[NET] <icsa_ike|15> sending packet: from 205.160.10.1[500] to
1.1.4.1[500] (432 bytes)
Mar 15 03:22:14 12[NET] [VNP 0] received an IPv4-mapped IPv6 packet
Mar 15 03:22:14 72[NET] <icsa_ike|15> received packet: from 1.1.4.1[500] to
205.160.10.1[500] (465 bytes)
Mar 15 03:22:14 72[ENC] <icsa_ike|15> parsed IKE_SA_INIT response 0 [ SA KE No
N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
Mar 15 03:22:14 72[IKE] <icsa_ike|15> 1.1.4.1[500]->205.160.10.1[500]: [ SA KE No
N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
Mar 15 03:22:14 72[IKE] <icsa_ike|15> received 1 cert requests for an unknown ca
Mar 15 03:22:14 72[IKE] <icsa_ike|15> authentication of '205.160.10.1' (myself)
with pre-shared key
Mar 15 03:22:14 72[IKE] <icsa_ike|15> establishing CHILD_SA icsa_tunnel
Mar 15 03:22:14 72[ENC] <icsa_ike|15> generating IKE_AUTH request 1 [ Idi
N(INIT_CONTACT) IDr AUTH N(ESP_TFC_PAD_N) SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) ]
Mar 15 03:22:14 72[IKE] <icsa_ike|15> 205.160.10.1[500]->1.1.4.1[500]: [ IDi
N(INIT_CONTACT) IDr AUTH N(ESP_TFC_PAD_N) SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) ]
Mar 15 03:22:14 72[NET] <icsa_ike|15> sending packet: from 205.160.10.1[500] to .
1.1.4.1[500] (256 bytes)
Mar 15 03:22:14 12[NET] [VNP 0] received an IPv4-mapped IPv6 packet
Mar 15 03:22:14 84[NET] <icsa_ike|15> received packet: from 1.1.4.1[500] to
205.160.10.1[500] (80 bytes)
Mar 15 03:22:14 84[ENC] <icsa_ike|15> parsed IKE_AUTH response 1 [ N(AUTH_FAILED) ]
Mar 15 03:22:14 84[IKE] <icsa_ike|15> 1.1.4.1[500]->205.160.10.1[500]: [
N(AUTH_FAILED) ]
Mar 15 03:22:14 84[IKE] <icsa_ike|15> received AUTHENTICATION_FAILED notify error
```

Security Testing

The IPSEC Product demonstrated resistance to a suite of IKEv2/IPSEC related attacks including some acquired and others developed by ICSA Labs such as traffic with malformed packets, spoofed and unprotected IKEv2 messages, and denial of service (DoS) attacks.

No configuration changes or fixes were required to protect the product under test from these security-related attacks.

Authority

This report is issued by the authority of the General Manager, ICSA Labs. Tests are performed under normal operating conditions.

Darren Hartman

Darren Hartman, General Manager, ICSA Labs

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For over 30 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

www.icsalabs.com

A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help futureproof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

a10networks.com