IPSEC Certification Testing Report
Version 3.1 Basic

A10 Networks
A10 Networks Thunder Series

January 8, 2021

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 nearly 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 the requirements below.

The following is a summary of ICSA Labs IPSEC Version 3.1 Basic requirements against which the product was tested:

- The Candidate IPSEC Product must be a generally available product and must be interoperable (negotiation, establishment, and rekeying of SAs) with other independent implementations.
- The Candidate IPSEC Product must be in compliance with a specific subset of requirements defined in the IETF IPSEC related RFCs.
- The Candidate IPSEC Product must be in compliance with a specific subset of requirements defined in the IETF IKEv2 related RFCs.
- The Candidate IPSEC Product must implement cryptographic algorithms without security-degrading mistakes.
- The Candidate 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 Candidate IPSEC Product must have the ability to log the required data for IKEv2 negotiation failures and other administrative changes.
- The Candidate IPSEC Product must provide cryptographically-protected remote administration.

Summary of Findings

With the successful testing of the TH-5330S model, the A10 Network Thunder Series satisfied all of the mandatory certification testing requirements to retain ICSA Labs IPSEC Version 3.1 Basic Certification.

Certification Maintenance

The Candidate 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 Candidate IPSEC Product to have its certification revoked:

1. The Candidate IPSEC Product vendor withdraws from the ICSA Labs IPSEC Certification Program.
2. The product fails periodic testing and the Candidate 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 Candidate 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 Candidate IPSEC Product, unless otherwise noted.

Hardware

A10 Networks provided the following product for testing:

- **TH-5330S**

Software

Testing was successfully completed with version **5.1.0-P5 build 66**.

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:

Thunder 840	Thunder 940	Thunder 1040	Thunder 3040
Thunder 3230	Thunder 3350	Thunder 3430	Thunder 4430
Thunder 4435	Thunder 4440	Thunder 5330	Thunder 5430S
Thunder 5440	Thunder 5840	Thunder 5840-11	Thunder 5845
Thunder 6440	Thunder 7440	Thunder 7440-11	Thunder 7445
Thunder 7650	Thunder 14045	TH-ADC-for-Baremetal	vThunder

The most up-to-date list of IPSEC-certified A10 Network Thunder Series models are on the ICSA Labs Website at the URL below:

https://www.icsalabs.com/product/thunder-series-platform

Test Configuration

ICSA Labs installed and configured the Candidate 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, *ACOS 5.1.0-P3 Configuring IPsec VPN,* from A10 Networks*.*

- After completing the steps specified in the *Basic IPsec VPN Deployment using the GUI* section, 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* step.
- 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 Candidate 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.

Security Vendor	Product Name	Product Version
F5	BIG-IP i10800	15.0.1 Build 0.0.11
Fortinet	FortiGate	v6.4.0 build1579 (GA)

Product interoperability was additionally tested successfully with the open source implementation of strongSwan (https://strongswan.org).

Note: The initial version submitted for testing, 5.1.0-P4 build 46, did not properly interoperate with other implementations that did not include an IKEv2 IDr payload in the IKE_AUTH exchange when acting as the IKE initiator. ICSA Labs subsequently tested version 5.1.0-P5 build 66. This version interoperated successfully with all implementations listed in the above table.

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. ICSA Labs confirmed the use of strong ciphers for remote administrative traffic.

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 level 3
#  show vpn log follow
```

Below is an example of how the TH-5330S logs an IKE failure due to an mismatched pre-shared key settings:

```
Dec 27 09:55:56 60[IKE] <icsatunn|1036> initiating IKE_SA icsatunn[1036] to 1.1.4.1
Dec 27 09:55:56 60[ENC] <icsatunn|1036> generating IKE_SA_INIT request 0 [ SA KE No
N(NATD_S_IP) N(NATD_D_IP) ]
```

```
Dec 27 09:55:56 60[IKE] <icsatunn|1036> 205.160.40.5[500]->1.1.4.1[500]: [ SA KE No
N(NATD_S_IP) N(NATD_D_IP) ]
Dec 27 09:55:56 60[NET] <icsatunn|1036> sending packet: from 205.160.40.5[500] to
1.1.4.1[500] (432 bytes)
Dec 27 09:55:56 61[NET] <icsatunn|1036> received packet: from 1.1.4.1[500] to
205.160.40.5[500] (465 bytes)
Dec 27 09:55:56 61[ENC] <icsatunn|1036> parsed IKE_SA_INIT response 0 [ SA KE No
N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
Dec 27 09:55:56 61[IKE] <icsatunn|1036> 1.1.4.1[500]->205.160.40.5[500]: [ SA KE No
N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
Dec 27 09:55:56 61[IKE] <icsatunn|1036> received 1 cert requests for an unknown ca
Dec 27 09:55:56 61[IKE] <icsatunn|1036> authentication of '205.160.40.5' (myself)
with pre-shared key
Dec 27 09:55:56 61[IKE] <icsatunn|1036> establishing CHILD_SA icsavtunn
Dec 27 09:55:56 61[ENC] <icsatunn|1036> 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) ]
Dec 27 09:55:56 61[IKE] <icsatunn|1036> 205.160.40.5[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) ]
Dec 27 09:55:56 61[NET] <icsatunn|1036> sending packet: from 205.160.40.5[500] to
1.1.4.1[500] (256 bytes)
Dec 27 09:55:56 62[NET] <icsatunn|1036> received packet: from 1.1.4.1[500] to
205.160.40.5[500] (80 bytes)
Dec 27 09:55:56 62[ENC] <icsatunn|1036> parsed IKE_AUTH response 1 [ N(AUTH_FAILED)
]
Dec 27 09:55:56 62[IKE] <icsatunn|1036> 1.1.4.1[500]->205.160.40.5[500]: [
N(AUTH_FAILED) ]
Dec 27 09:55:56 62[IKE] <icsatunn|1036> received AUTHENTICATION_FAILED notify error
Dec 27 09:55:56 62[KNL] <icsatunn|1036> unable to delete SAD entry with SPI 10233eed
```

Security Testing

The Candidate 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.

Sebastien Mazas, 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 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) enables service providers, cloud providers and enterprises to ensure their 5G networks and multi-cloud applications are secure. With advanced analytics, machine learning and intelligent automation, business-critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers in 117 countries worldwide.

a10networks.com