# IPSEC Certification Testing Report
# IKEv2 Basic
### Criteria Version 3.0

## A10 Networks
## A10 Networks Thunder Series

January 10, 2019

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

# A10 Networks – A10 Networks Thunder Series
# IPSEC Certification Testing Report

## Table of Contents

Copyright © 2019 ICSA Labs. All rights reserved.

# A10 Networks – A10 Networks Thunder Series
# IPSEC 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 25 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 3.0 is based on the Internet Key Exchange (IKE), IKE version 2 (IKEv2), and IPSEC protocols.

The following is a summary of the IPSEC 3.0 BASIC requirements against which the product was tested:

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

Copyright © 2019 ICSA Labs. All rights reserved.

## A10 Networks – A10 Networks Thunder Series
## IPSEC Certification Testing Report

### Summary of Findings

The A10 Networks Thunder Series satisfied all the mandatory requirements to achieve ICSA Labs IPSEC Version 3.0 IKEv2 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

- Thunder 5330

### Software

Testing was successfully completed with version 4.1.1-P6 Build 62

### 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.

Copyright © 2019 ICSA Labs. All rights reserved.

# A10 Networks – A10 Networks Thunder Series
# IPSEC Certification Testing Report

## Product Family Members

| | | | | |
|---|---|---|---|---|
| **THUNDER 840** | **THUNDER 940** | **THUNDER 1030S** | **THUNDER 1040** | **THUNDER 3030S** |
| **THUNDER 3230** | **THUNDER 3430** | **THUNDER 4440** | **THUNDER 3430** | **THUNDER 4440** |
| **THUNDER 5440** | **THUNDER 5840** | **THUNDER 5840-11** | **THUNDER 6440** | **THUNDER 7440** |

## 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 ***A10 Thunder Series and AX Series—Configuring IPsec VPN*** guidance document.

- The IPsec protocols, and specifically the IKEv2 protocol, allow for narrowing of traffic selectors to specify an exact set of traffic that is protected by IPsec. During testing, ICSA Labs found that the A10 Thunder model under test could be configured to narrow traffic selectors in the VPN Tunnel configuration; however, the IPsec policy was not enforced without also configuring firewall rules that match the traffic selectors. With both IPsec policy and firewall rules in place, the A10 Thunder properly interoperated with other IPsec implementations and enforced the policy as intended.

Copyright © 2019 ICSA Labs. All rights reserved.

## Detailed Findings

### IKEv2/IPSEC Interoperability

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

| Vendor | Product Name | Product Version |
|---|---|---|
| Fortinet, Inc. | FortiGate 501E | 6.0.3 build 0200 (GA) |

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

### 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

No implementation errors were found during testing of the A10 Thunder Series. ICSA Labs confirmed that explicit Initialization Vectors (IVs) were generated properly.

### 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.

### Logging

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

For most events, logging is enabled in the GUI under the “`system`” heading and “`logging`” sub-heading. To capture IKE negotiation logs ICSA Labs used the following commands:

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

Copyright © 2019 ICSA Labs. All rights reserved.

## 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 command line interface was also verified. In both cases, ICSA Labs confirmed the use of strong ciphers by the product under test.

# A10 Networks – A10 Networks Thunder Series
# IPSEC Certification Testing Report

## Authority

This report is issued by the authority of the General Manager, ICSA Labs.  Tests are done 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 more than 25 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, a leader in Application Networking, helps organizations of all sizes to accelerate, optimize and secure their applications. A10's primary market for Application Delivery Networking is driven by the massive growth of global IP traffic and expected to double to $2.9 billion in four years (source: Gartner). A10 was named one of the fastest growing private companies in North America by the Deloitte Fast 500™ and Inc. 500. Headquartered in San Jose, CA, A10 has offices in over 22 countries, over 500 employees and is profitable with a track record of consistent quarterly revenue growth.

www.a10.com

Copyright © 2019 ICSA Labs.   All rights reserved.