IPSEC Enhanced Certification Testing Report
IKEv2 Criteria Version 3.1

Fortinet
FortiGate Consolidated Security Platforms

May 8, 2020

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

Table of Contents

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

With models ranging from those suited for small businesses to models designed for large enterprises, service providers and carriers, FortiGate Consolidated Security Platforms combine the FortiOS™ security operating system with FortiASIC processors and other hardware to provide a comprehensive and high-performance array of security and networking functions.

FortiGate Consolidated Security Platforms provide cost-effective, comprehensive protection against network, content, and application-level threats - including complex attacks favored by cybercriminals - without degrading network availability and uptime. FortiGate platforms incorporate sophisticated networking features, such as high availability (active/active, active/passive) for maximum network uptime, and virtual domain capabilities to separate various networks requiring different security policies.

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 both its "BASIC" and "ENHANCED" requirements. These sets of requirements are summarized below.

The following is a summary of the IPSEC 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 fatal or 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.

The following is a summary of the IPSEC 3.1 ENHANCED requirements against which Fortinet additionally opted to be tested:

- The Candidate IPSEC Product must support RSA Signature authentication.
- The Candidate IPSEC Product must support a secure mechanism for installation of X.509 certificates.
- The Candidate IPSEC Product must properly execute certificate validation and provide for automatic retrieval of certificate revocation information.
- The Candidate IPSEC Product must interoperate with dynamically addressed peers with the use of digital certificate based authentication.

Summary of Findings

Following successful testing of the FortiGate VM64 virtual appliance, the FortiGate Consolidated Security Platforms satisfied all of the mandatory certification testing requirements to retain ICSA Labs IPSEC Version 3.1 IKEv2 ENHANCED 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

Fortinet provided the following product for ICSA Labs IPSEC IKEv2 ENHANCED certification testing:

- **FortiGate VM64 virtual appliance**

Software

Testing was successfully completed with version v6.2.2 build 1010(GA)

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 FortiGate Consolidated Security Platforms that are ICSA Labs IPSEC Version 3.1 IKEv2 ENHANCED Certified include the following:

FortiGate/ FortiWifi 30E	FortiGate/FortiWifi 51E	FortiGate/FortiWifi 61E	FortiGate 81E/FortiWifi 81E-POE	FortiGate/FortiWifi 91E
FortiGate 100E/101E	FortiGate 100F/101F	FortiGate 200E/201E	FortiGate 300D	FortiGate 300E/301E
FortiGate 400E/401E	FortiGate 500E/501E	FortiGate 600D	FortiGate 600E/601E	FortiGate 800D
FortiGate 1000D	FortiGate 1100E/1101E	FortiGate 1200D	FortiGate 1500D	FortiGate 2000E
FortiGate 2200E/2201E	FortiGate 2500E	FortiGate 3000D	FortiGate 3300E/3301E	FortiGate 3700D
FortiGate 3800D	FortiGate 3960E	FortiGate 3980E	FortiGate 5000	FortiGate 6300E/6301E
FortiGate 6500E/6501E	FortiGate 7030E	FortiGate 7040E	FortiGate 7060E	FortiGate VAs

The most up-to-date list of IPSEC-certified FortiGate Consolidated Security Platforms are on the ICSA Labs Website at the URL below:

https://www.icsalabs.com/product/fortigate-multi-threat-security-platforms

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 Fortinet guidance information available on the Fortinet Support site:
  - ***docs.fortinet.com/product/fortigate/6.2***.
- A summary to configure a site-to-site VPN with a third party gateway:

  IPsec Tunnels > Create New
  - Enter Name
  - Select Custom
  - Next
  - Enter Remote Gateway Static IP Address
  - Select External Interface
  - Enable Local Gateway and select Primary IP
  - Select Pre-shared Key or Signature & configure related items
  - IKE Version 2
  - Verify/limit Phase 1 Proposal, e.g. AES256, SHA256, DH Group 14
  - Enter lifetime
  - Enter New Phase 2 – Local and Remote addresses, i.e. local/remote subnets
  - Advanced…Verify/limit Phase 2 Proposal, e.g. AES256, SHA256 (DH Group 14 if enabling PFS)
  - Local Port, Remote Port, Protocol = All
  - Enter lifetime

  Policy & Objects > IPv4 Policy > Create New
  - Enter Name for vpn outbound policy
  - Incoming Interface = Internal
  - Outgoing Interface = <IPsec Tunnel created above>
  - Source = add/choose local subnet
  - Destination = add/choose local subnet
  - Service = ALL
  - Action = ACCEPT, Inspection Mode = Flow-based
  - NAT disabled
  - Set Log options as needed
  - Enable this policy (Note, FG will initiate IKE soon after saving policy)
  - Create New policy for vpn inbound, swapping Interfaces and Source/Destination settings

  Network > Static Routes > Create New
  - Destination = Subnet (or Named Address if Addresses Object was created with Show route configuration option enabled), enter Remote subnet

- Interface = <IPsec Tunnel created above>
- OK
- Create New route with Interface = Blackhole and Administrative Distance = 255 (prevents traffic passing through FG when VPN is down)

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
F5	BIG-IP i10800	V15.0.1 bld 0.0.11

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

Administration

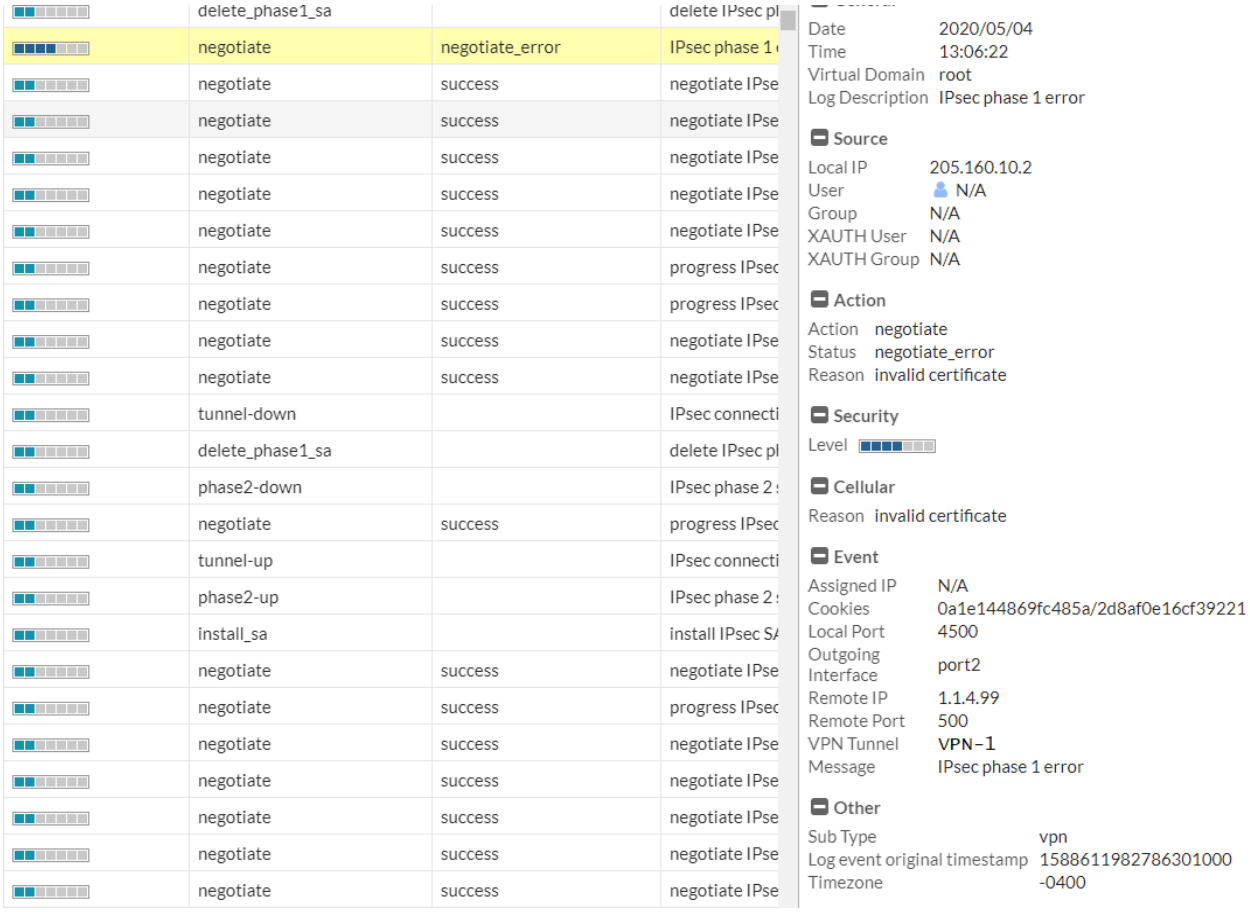
ICSA Labs verified that secure remote access was supported. Administration was performed using a web browser via HTTPS access. ICSA Labs confirmed the use of strong ciphers for remote administrative traffic.

Logging

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

To view the required data related to failed IKE negotiatiations, enable Log Settings > Event Logging: VPN activity events. Navigate to Log & Report > Events, select VPN Events.

Below is an example of how Fortinet logs an IKE failure due to an invalid peer certificate sent in the IKE exchange:



	delete_phase1_sa		delete IPsec pl
	negotiate	negotiate_error	IPsec phase 1
	negotiate	success	negotiate IPse
	negotiate	success	negotiate IPse
	negotiate	success	negotiate IPse
	negotiate	success	negotiate IPse
	negotiate	success	negotiate IPse
	negotiate	success	progress IPsec
	negotiate	success	progress IPsec
	negotiate	success	negotiate IPse
	negotiate	success	negotiate IPse
	tunnel-down		IPsec connecti
	delete_phase1_sa		delete IPsec pl
	phase2-down		IPsec phase 2
	negotiate	success	progress IPsec
	tunnel-up		IPsec connecti
	phase2-up		IPsec phase 2
	install_sa		install IPsec SA
	negotiate	success	negotiate IPse
	negotiate	success	progress IPsec
	negotiate	success	negotiate IPse
	negotiate	success	negotiate IPse
	negotiate	success	negotiate IPse
	negotiate	success	negotiate IPse
	negotiate	success	negotiate IPse

Figure 1. Failed IKE Log Entry

Enhanced

In addition to the BASIC requirements that must be met by all ICSA Labs certified IPSEC products, the FortiGate Consolidated Security Platforms additionally met the ENHANCED requirements as well.

- The FortiGate supports RSA Signature IKE authentication.
- The FortiGate supports a secure method for installing an X.509 certificate from an external Certification Authority.
- Certificates were installed using a manual enrollment method.
- The FortiGate supports methods to retrieve certificate revocation list (CRL) information. CRL retrieval via HTTPS was verified.
  - The FortiGate properly validates peer certificates and CRLs. In addition to valid scenarios, proper behavior in the following cases was verified:
    - The peer was configured with an expired certificate
    - The peer was configured with a revoked certificate
    - The peer sent a certificate with an invalid signature

- The retrieved CRL had expired, i.e. Next Update field was in the past
- The retrieved CRL had an invalid signature

Configuration Notes:

A summary to install certificates and CRL:

- Install CA certificate
  - Navigate to: System > Certificates
  - Select: Import > CA Certificate
  - Upload CA certificate
- Generate certificate request and install local certificate
  - Navigate to: System > Certificates
  - Select: + Generate
  - Enter values and OK
  - Select newly created certificate request and download
  - Import > Local Certificate
- Configure CRL
  - Navigate to: System > Certificates
  - Import > CRL

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 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 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.

www.icsalabs.com

Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks number one in the most security appliances shipped worldwide and more than 450,000 customers trust Fortinet to protect their businesses.

fortinet.com