Firewall

Certification Testing Report

Fortinet
FortiGate Consolidated Security Platforms

Tested against these standards

ICSA Labs Firewall Certification Criteria Baseline Module – Version 4.2
ICSA Labs Firewall Certification Criteria Corporate Module – Version 4.2

September 8, 2022

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

Table of Contents

Executive Summary 1
Introduction 1
Summary of Findings 1
Product Overview 1
Scope of Assessment 1
Continuous Deployment and Spot Checks 1
Tested Firewall Product Components 2
Hardware 2
Software 2
Documentation 2
Product Family Members 2
Installation and Configuration 2
Required Services Security Policy Transition 3
Expectation 3
Results 3
Logging 4
Expectation 4
Results 4
Administration 4
Expectation 4
Results 4
Persistence 5
Expectation 5
Results 5
Documentation 5
Expectation 5
Results 5
Functional and Security Testing 5
Expectation 5
Results 6
Criteria Violations and Resolutions 6
Introduction 6
Results 6
ICSA Labs Certified Firewalls 6
Authority 7

Executive Summary

Introduction

The goal of ICSA Labs certification testing is to 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 measuring product security, compliance and performance.

Summary of Findings

Following rigorous security testing at ICSA Labs, the FortiGate 400E satisfied all of the firewall security testing requirements in both the ICSA Labs baseline firewall and ICSA Labs corporate firewall testing standards. As a result, both the FortiGate 400E and the entire list of models comprising the e Fortinet Consolidated Security Platforms family retained ICSA Labs Firewall Certification having met all of the testing requirements.

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

ICSA Labs tests firewall products against its industry-approved set of testing criteria. Over time, this set of testing criteria became an industry standard. Testing requirements evolved with input from a consortium of firewall vendors, end users, and ICSA Labs. The present iteration of *The Firewall Certification Criteria* is version 4.2*.*

Continuous Deployment and Spot Checks

Following security testing by ICSA Labs, all tested firewall products remain continuously deployed at the labs for the length of the testing contract. When relevant new attacks and vulnerabilities are discovered, all deployed firewall models may be periodically checked to ensure they provide the requisite protection. In the event that any firewall is found susceptible to new attacks or vulnerabilities during a check, ICSA Labs works with the security product vendor to resolve the shortcomings in order for the product to maintain its ICSA Labs Firewall Certification.

Tested Firewall Product Components

Hardware

Fortinet provided the following model to ICSA Labs for firewall security certification testing:

- FortiGate 400E

Software

Testing began and successfully completed with firmware version 7.0.6 build0366.

Documentation

To satisfy documentation requirements, Fortinet provided ICSA Labs with the following document in order to assist in the installation, configuration, and administration of their firewall product:

- FortiOS 7.0.6 Administration Guide

Product Family Members

ICSA Labs Corporate Firewall Certification extends beyond the most recently tested model (identified in the “Hardware” section above) to the other members of the FortiGate Consolidated Security Platforms Family. Therefore all of the models from the family listed below are ICSA Labs Certified Firewalls. For that reason, ICSA Labs periodically tests other physical and/or virtual models in the family. Finally, note that any models found on the security vendor’s datasheet that is neither listed below nor listed on the ICSA Labs certified product list is not ICSA Labs Certified:

FortiGate 30D-Rugged	**FortiGate/FortiWifi 30E**	**FortiGate 35D-Rugged**	**FortiGate 40F**
FortiGate/FortiWifi 51E	**FortiGate 60D-Rugged**	**FortiGate 60F**	**FortiGate 60F-Rugged**
FortiGate 60F 3G/4G-Rugged	**FortiGate/FortiWifi 61E**	**FortiGate 70F**	**FortiGate 80F/81F**
FortiGate 81E/FortiWifi 81E-POE	**FortiGate 90D-Rugged**	**FortiGate/FortiWifi 91E**	**FortiGate 100E/101E**
FortiGate 100F/101F	**FortiGate 200E/201E**	**FortiGate 200F/201F**	**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 1800F/1801F**	**FortiGate 2000E**
FortiGate 2200E/2201E	**FortiGate 2500E**	**FortiGate 2600F/2601F**	**FortiGate 3000D**
FortiGate 3300E/3301E	**FortiGate 3400E/3401E**	**FortiGate 3600E/3601E**	**FortiGate 3700D**
FortiGate 3800D	**FortiGate 3960E**	**FortiGate 3980E**	**FortiGate 4200F/4201F**
FortiGate 4400F/4401F	**FortiGate 5000**	**FortiGate 6300E/6301E**	**FortiGate 6500E/6501E**
FortiGate7030E	**FortiGate 7040E**	**FortiGate 7060E**	**FortiGate VM**

Installation and Configuration

Firewall products can be configured different ways; therefore, ICSA Labs typically makes many configuration related decisions prior to adding a security policy to the firewall. Because ICSA Labs attempts to exploit the product under test, configuration decisions were made in an attempt to make exploitation less likely.

ICSA Labs installed and configured the security vendor's product following the firewall product documentation. Any special configuration changes or deviations from the documentation that were necessary to execute a test or meet a requirement are documented in this section.

ICSA Labs configured the FortiGate 400E in routing mode for both inbound and outbound traffic. Additional GUI and CLI configurations were performed to prepare for testing:

- Log traffic session start

```
WebGUI > Policy & Objects > Firewall Policy > Right click policy > edit in CLI > "set
logtraffic-start enable" > end
```

- Prevent FTP Bounce Attacks

```
WebGUI > Security Profiles > Intrusion Prevention > Create New > Name the IPS Sensor >
Create New IPS Signature > Set Type to Signature > Set Action to Block > Set Status to
Enable > Search for "FTP.Protocol.Bounce.Attack" > Right click > Add Selected > Ok >
Ok > Enable IPS checkbox on Firewall Rules and select the created IPS Sensor
```

- Block Cert vulnerability 328867, an FTP state-related exploit from traversing the firewall

```
WebGUI > Security Profiles > Intrusion Prevention > Create New > Name the IPS Sensor >
Create New IPS Signature > Set Type to Signature > Set Action to Block > Set Status to
Enable > Search for "Fakeftpclient.Attack" > Right click > Add Selected > Ok > Ok >
Enable IPS checkbox on Firewall Rules and select the created IPS Sensor
```

Required Services Security Policy Transition

Expectation

Each phase of firewall testing is performed predominantly while enforcing a particular security policy. Firewall products must be configurable to minimally enforce a security policy such as the one specified in *The Modular Firewall Certification Criteria,* referred to as the Required Services Security Policy or RSSP. The RSSP permits a set of common Internet services inbound and outbound while dropping or denying all other network traffic.

Results

ICSA Labs performed port scans followed by additional scans and other tests to ensure that the security vendor's product was indeed configured according to the RSSP and that no other TCP, UDP, ICMP, or other IP protocol traffic was permitted to or through the firewall in either direction.

After performing the scans mentioned above, ICSA Labs verified that the firewall properly handled all permitted outbound and inbound service requests. ICSA Labs also confirmed that no other traffic traversed the firewall in either direction that would violate the security policy.

ICSA Labs determined through testing that the FortiGate 400E met all the security policy transition requirements.

Logging

Expectation

Firewalls destined for enterprise and government organizations as well as firewalls provided by managed security services providers need to provide an extensive logging capability. This explains why the breadth and depth of ICSA Labs firewall log testing is so extensive.

ICSA Labs tested the logging functionality provided by the firewall product under test ensuring that all permitted and denied traffic was logged. Analysts in the lab sent traffic both to and (attempted to send traffic) through the product. Other events that must be logged are system startups, time changes, access control rule changes, and administrative login attempts. ICSA Labs typically configures firewall products to send log data for logged events to an external server such as a syslog server. For all logged events ICSA Labs verified that the appropriate, required log data was recorded.

Results

With any Fortinet Consolidated Security Platform Firewall, including the FortiGate 400E, logs can be retrieved locally via the web UI. In addition, logged events can be sent to an external server such as a syslog server. For this test cycle, ICSA Labs configured the tested model to log remotely.

The following depicts how the FortiGate 400E logs an attempted FTP Bounce Attack:

```
Sep  6 10:58:17 205.160.45.254 date=2022-09-06 time=11:00:26 devname="FortiGate-400E"
devid="FG4H0ETB21903292" eventtime=1662476426946979598 tz="-0400" logid="0419016384" type="utm"
subtype="ips" eventtype="signature" level="alert" vd="root" severity="low" srcip=205.160.45.66
srccountry="United States" dstip=205.160.40.66 dstcountry="United States" srcintf="port1"
srcintfrole="lan" dstintf="port2" dstintfrole="wan" sessionid=87375 action="dropped" proto=6
service="FTP" policyid=3 poluuid="36da85b8-0f67-51ed-42d5-01d00a8e8e30" policytype="policy"
attack="FTP.Protocol.Bounce.Attack" srcport=42527 dstport=21 direction="outgoing"
attackid=109445133 profile="icsa" ref="http://www.fortinet.com/ids/VID109445133"
incidentserialno=192937990 msg="ftp_decoder: FTP.Protocol.Bounce.Attack, ip 205.160.40.122 !=
205.160.45.66" crscore=5 craction=32768 crlevel="low"
```

ICSA Labs determined through testing that the FortiGate 400E met all the logging requirements.

Administration

Expectation

Firewall products often have more than a single method by which administration is possible. Whether the product can be administered remotely using vendor provided administration software, from a web browser based interface, via some non-networked connection such as a serial port, or some other means, authentication must be possible before access to administrative functions is granted. ICSA Labs tested not only that authentication mechanisms existed but also that they could not be bypassed and that remote administration traffic was encrypted.

Results

ICSA Labs remotely administered the FortiGate 400E in the lab from the private network using the available web-based GUI via HTTPS. Attempts to bypass the authentication mechanism for all means of administration were unsuccessful.

ICSA Labs determined through testing that the FortiGate 400E met all the administration requirements.

Persistence

Expectation

Power outages, electrical storms, and inadvertent power losses should not cause the firewall to lose valuable information such as the remote administration configuration, security policy being enforced, log data, time and date, and authentication data. This section documents the findings of ICSA Labs testing of the firewall product against the persistence requirements.

Results

The FortiGate 400E continued to maintain its configuration, settings, and data following a forced power outage. Similarly, the product continued to enforce the configured security policy following the outage.

ICSA Labs determined through testing that the FortiGate 400E met all the persistence requirements.

Documentation

Expectation

ICSA Labs expects firewall documentation to be accurate and applicable to the version tested. The documentation should minimally provide appropriate guidance for installation, configuration and administration.

Results

ICSA Labs determined that the documentation provided was adequate and accurate for the purposes of product installation and administration.

The documentation provided by Fortinet met all of the documentation requirements.

Functional and Security Testing

Expectation

Once configured to enforce a security policy an ICSA Labs certified firewall must properly permit the services allowed by that policy. In this case, “properly” means that the service functions correctly. The firewall must be capable of preventing well-known, potentially harmful behavior found in some network protocols while at the same time maintaining compliance with applicable network protocol standards in all other ways. In the event of a conflict between these two things, a firewall tested and certified by ICSA Labs must defer to providing increased security. During functional testing ICSA Labs checked to ensure proper protocol behavior for the permitted services.

During security testing, ICSA Labs used commercial, in-house, and freely available testing tools to attack and probe the firewall. ICSA Labs used these tools to attempt to defeat or circumvent the security policy enforced. Additionally, using Denial-of-Service and fragmentation attacks ICSA Labs attempted to overwhelm, bypass or otherwise defeat the enforced security policy.

Since there is overlap between functional and security testing, the results of both phases of testing are presented here.

Results

ICSA Labs determined through testing that the FortiGate 400E and, by extension, the entire Fortinet Consolidated Security Platforms family met all of the ICSA Labs functional and security testing criteria requirements.

Criteria Violations and Resolutions

Introduction

In the event that ICSA Labs uncovers criteria violations while testing a firewall product, the security vendor must make repairs before testing is successfully completed and certification granted. The section that follows documents all criteria violations discovered during testing.

Results

No firewall security testing criteria violations or other firewall product shortcomings were found during the test cycle.

ICSA Labs Certified Firewalls

Because the FortiGate 400E passed all of the firewall security test cases performed by ICSA Labs and as the tested product met the entire set of testing criteria requirements, ICSA Labs is pleased to state that both the FortiGate 400E and the other models comprising the Fortinet Consolidated Security Platforms family retained ICSA Labs Corporate Firewall Certification.

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 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.

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.

https://www.fortinet.com/