2019

Network Intrusion Prevention Systems

Certification Testing Report

Fortinet, Inc.
Fortinet Consolidated Security Platforms

Tested against this standard

ICSA Labs Network IPS Certification Testing Criteria v.2.0

July 12, 2019

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

ICSA Labs Network Intrusion Prevention Systems
Certification Testing Report

ICSA labs
An Independent Division of Verizon

FORTINET

Fortinet Consolidated Security Platforms

www.fortinet.com/products/ips.html

Model Tested: FortiGate IPS 600D

Firmware: v.6.0.4 build 231 (GA)

ICSA labs
CERTIFIED NETWORK IPS

Certified
Since November 2006

Summary of Test Results

Exploit Prevention Efficacy	Protects from exploits aimed at test set			100%
	Same + 512 Mbps of background traffic			100%
	Same + common evasion techniques			100%
DoS Mitigation Efficacy	Mitigates denial of service attacks in test set			100%
	Same + 358 Mbps of background traffic			100%
Platform Security	Self-protection against exploits including:			
	SSL-Heartbleed	✓	With background traffic	✓
	SSL-CSS-Injection	✓		✓
	SSL-Known-Key	✓		✓
	SSL-Poodle	✓		✓
	Various DoS Attacks	✓		✓
Admin	Secure?			✓
	Protocol?			TLS-1.2
	Strong NIST-approved Ciphers?			✓
Logging	To remote server?			✓
	Logs addition of any new admin user?			✓
	Logs security policy changes?			✓
	Logs blocked traffic?			✓
	Logs permitted traffic?			✓

About ICSA Labs

For thirty years, ICSA Labs has performed independent, third-party security certification testing of computer and network security products, beginning with anti-malware testing in 1991.

Network IPS Security Certification Testing

ICSA Labs began testing network intrusion prevention systems (IPS) in 2006. Since then, the focus of ICSA Labs Network IPS testing is determining how well the security vendor's product protects against exploits targeting known vulnerabilities.

More specifically, ICSA Labs network IPS testing confirms that tested products block all attacks aimed at an evolving set of known vulnerabilities in enterprise software. As the vulnerabilities in the test set are at least a few months old, ICSA Labs requires that certified products prevent 100% of the exploits targeting them.

> "ICSA Labs network IPS testing confirms that tested products block all attacks aimed at an evolving set of known vulnerabilities in enterprise software."

Because real world attacks do not happen on a quiescent network, ICSA Labs tests with an appropriate level of background traffic using various mixes of enterprise network traffic. Also tested are evasion techniques, denial of service (DoS) attacks, platform security of the product itself, logging, secure administration, and administrative functions.

Certified Product Models

As ICSA Labs periodically tests other models in the series, ICSA Labs Network IPS Certification extends beyond the most recently tested model (in **bold** below) to the other members of the FortiGate Consolidated Security Platform:

FortiGate/ FortiWifi 30E
FortiGate/ FortiWifi 51E
FortiGate/ FortiWifi 61E
FortiGate 81E/ FortiWifi 81E-POE
FortiGate/ FortiWifi 91E
FortiGate 100F
FortiGate 101E
FortiGate 101F
FortiGate 200E
FortiGate 300E
FortiGate 301E
FortiGate 401E
FortiGate 501E
FortiGate 600D
FortiGate 601E
FortiGate 800D
FortiGate 1000D
FortiGate 1200D
FortiGate 1500D
FortiGate 2000E
FortiGate 2500E
FortiGate 3000D
FortiGate 3700D
FortiGate 3800D
FortiGate 3960E
FortiGate 3980E
FortiGate 5000
FortiGate 6000
FortiGate 7030E
FortiGate 7040E
FortiGate 7060E

Background Traffic

During this network IPS test cycle, ICSA Labs used the Spirent CyberFlood tool to create non-malicious, legitimate background traffic filling 512 Mbps of bandwidth. Though the FortiGate IPS 600D has 1 Gbps interfaces, ICSA Labs intentionally set the throughput to this more reasonable level. ICSA Labs subsequently tested how well the FortiGate network IPS detects attacks aimed at the vulnerability set while simultaneously sending legitimate network traffic.

In testing, the labs used the Spirent CyberFlood tool to generate attack traffic and background traffic. The FortiGate IPS 600D was tested with a mix of HTTP, HTTPS, Telnet, SMTP and DNS as background traffic (refer to Fig. 1 below) while attempting to pass the attacks.

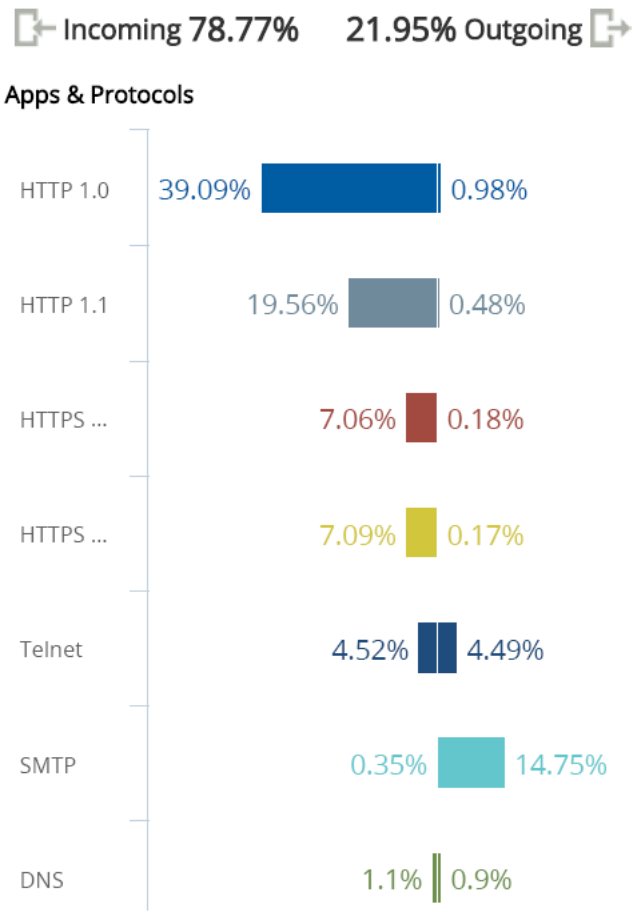

Fig. 1 Background Traffic Mix

Vulnerability Coverage Protection

In testing, the FortiGate IPS 600D provided 100% coverage protection against exploits aimed at the following set of known vulnerabilities found in enterprise software. The vulnerabilities in the test set listed below are presented by year and then by CVE ID.

2018-0802	2018-0835	2018-0883	2018-0891	2018-2616
2018-4878	2018-4901	2018-4904	2018-4910	2018-5093
2018-5378	2018-5379	2018-5381	2018-6356	2018-6389
2018-7183	2018-7187	2018-7284	2018-7285	2018-7286
2017-0004	2017-0143	2017-10151	2017-1092	2017-11213
2017-11511	2017-12617	2017-1274	2017-14461	2017-14803
2017-17439	2017-3248	2017-3599	2017-5112	2017-5340
2017-5638	2017-5689	2017-6950	2017-7269	2017-7494
2017-7529	2017-7546	2017-7991	2017-8717	2017-8718
2017-8779	2017-8917	2017-8961	2017-8994	2017-9788
2017-9800				
2016-1000110	2016-4385	2016-5360	2016-5792	2016-5803
2016-7250	2016-7478	2016-8204	2016-8705	2016-8869
2016-9054	2016-9941			

FortiGate IPS 600D
100% protection against tested attacks

Vulnerabilities Tested
63

High CVSS Base Scores
✓

Remotely Exploitable?
✓

Coverage Protection Tested With and Without Background Traffic?
✓

When choosing the vulnerabilities for the test set, a preference was given to server vulnerabilities; however, the test set does include a subset of client vulnerabilities as well. Because ICSA Labs requires 100% coverage protection to pass and attain (retain) ICSA Labs network IPS certification, the test set does not include new, 0-day vulnerabilities. Instead the test set typically (with a few exceptions) includes vulnerabilities between 6 months and about 2.5 years old. All selected vulnerabilities have high base CVSS scores. Some additional selection criteria are that the chosen vulnerabilities must be susceptible to network based attacks, have a low attack complexity required to exploit them, require no-or-low privileges, and require no user interaction.

Protocol	Client Incoming BW	Client Outgoing BW	Bytes Sent	Bytes Received	Not Blocked Transactions	Blocked Transactions	Attempted Transactions
NIPS VulnSet ...	6.27 Kbps	6.53 Kbps	293.66 KB	282.11 KB	0	85	86

Fig. 2 Attack Data

DoS Mitigation Testing

While the primary purpose of a network IPS device is to protect enterprises from remote, network-based attacks aimed at server and client vulnerabilities, ICSA Labs believes that a network IPS should also mitigate denial of service attacks. While in the midst of DoS attacks, the product is tested to ensure it continues to properly function. The tested product must both continue accepting new legitimate connections with minimal loss and continue to be administrable.

In DoS testing, ICSA Labs used the Spirent CyberFlood tool to generate two types of DoS attacks, Volumetric DDoS and Protocol DDoS attacks. The Volumetric DDoS Attack test is designed to simulate a large scale, bandwidth intensive DDoS attack, which would cause network congestion making the target unreachable. The Protocol DDoS Attack test simulates a protocol-based attack designed to cause state exhaustion on the target or intermediate network devices.

Volumetric DDoS Attack examples:

- **ICMP packet floods**
- **Malformed ICMP, UDP, IP and TCP packet floods**
- **UDP packet floods (with invalid payload data)**
- **Spoofed ICMP packets**

Protocol DDoS Attack examples:

- **SYN floods**
- **ACK floods**
- **RST floods**
- **TCP state exhaustion attacks**

In all cases, ICSA Labs tested to ensure that while under a DoS attack the FortiGate functioned properly and permitted valid traffic to pass freely with little loss. ICSA Labs found, as demonstrated in the results below that during DoS testing the product under test remained responsive, passed legitimate traffic, and blocked the DoS attack traffic. DoS attacks were mitigated by configuring and enabling an *IPv4 DoS Policy.*

Volumetric DDoS Attack Test Results

- **DDoS Attack Sent: 460.8 Mbps**
- **DDoS Attack Received: 0 bps**
- **HTTP Volume: 51.2 Mbps**
- **Successful HTTP Transactions: 97.03%**
- **HTTP Application Throughput: 57.12 Mbps**

Protocol DDoS Attack Test Results

- **DDoS Attack Sent: 153.6 Mbps**
- **DDoS Attack Received: 0 bps**
- **HTTP Volume: 358.4 Mbps**
- **Successful HTTP Transactions: 98.46%**
- **HTTP Application Throughput: 359.96 Mbps**

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.

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050

Fortinet, Inc.

Fortinet's mission is to deliver the most innovative, highest performing network security platform to secure and simplify your IT infrastructure. We are a leading global provider of network security appliances for carriers, data centers, enterprises and distributed offices. Because of our custom ASICs, hardware systems, network software, management capabilities and security research, we have a large, rapidly growing customer base, including the majority of the Fortune Global 100. Our market position and solution effectiveness has been widely validated by industry analysts, independent testing labs, business organizations, and the media worldwide. Our broad product line of complementary solutions goes beyond Network Security to help secure the extended enterprise.

www.fortinet.com

Fortinet, Inc.
899 Kifer Road
Sunnyvale, CA 94086