Firewall

Certification Testing Report

VMware
VMware SD-WAN Edge™ Series

Tested against these standards

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

April 6, 2022

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

Table of Contents

VMware – VMware SD-WAN Edge Series
Firewall Certification Testing Report

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, VMware SD-WAN Edge 620 and VMware SD-WAN Edge 3400 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, these two Edge models and the other models comprising the VMware SD-WAN Edge series attained ICSA Labs Firewall Certification.

Product Overview

VMware SD-WAN™ is a part of VMware's overall SASE solution. As one of the components of VMware SD-WAN, Edges are centrally managed, enterprise-grade appliances that offer secure, optimized connectivity to applications and services on- or off-cloud. VMware SD-WAN Edge supports zero-touch provisioning, deep application recognition, and performance assurance through Dynamic Multi-Path Optimization™ (DMPO) for fast and reliable branch access to the Internet and data centers. The built-in application-based, stateful firewall allows advanced traffic filtering and protects against network-based attacks.

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

VMware provided the following models to ICSA Labs for firewall security certification testing:

- VMware SD-WAN Edge 620
- VMware SD-WAN Edge 3400

Software

Testing began with firmware version 4.0.0 build R400-20200413-MH, and successfully completed on firmware version 5.0.1.0 build R5010-20220228-GA_94E5f0654.

Documentation

To assist with product installation, configuration, and administration and to satisfy the documentation requirements, VMware provided ICSA Labs with the following document:

- Orchestrator embedded Help UI

Product Family Members

ICSA Labs Corporate Firewall Certification extends beyond the most recently tested models (identified in the "Hardware" section above) to the other members of the VMware SD-WAN Edge series. Therefore, the entire Edge family listed below are ICSA Labs Certified Firewalls. For that reason, ICSA Labs periodically tests other physical and/or virtual models in the series. Finally, note that any model 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:

- Edge 5x0, 6x0, 8x0, 2000, 3x00 hardware series as well as Virtual Edge series

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 changes may have been 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 Edge 620 and Edge 3400 in routing mode for both inbound and outbound traffic. In addition to security policy rule changes, ICSA Labs made the following configuration changes to prepare the two models for testing:

- Turned "`Firewall Status`" and "`Stateful Firewall`" to "`On`" under the firewall tab of each VMware SD-WAN Edge appliance.
- Enabled "`Invalid TCP Flags`" to prevent packets with improper TCP flag combinations from traversing the VMware SD-WAN Edge appliances.

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.

Though only one mode needs to work properly to pass, ICSA Labs tests both active and passive mode FTP. Testing revealed that the VMware SD-WAN Edges only support passive mode FTP.

After performing the scans mentioned above, ICSA Labs found through testing that Edge 620 and Edge 3400 models did not initially handle all permitted outbound and inbound service requests properly. For details on what was corrected, please refer to the "Criteria Violations and Resolutions" section of this report.

After VMware addressed the issues reported by ICSA Labs and repairs were subsequently applied, the tested VMware SD-WAN Edges met all the security policy transition requirements.

Logging

Expectation

Firewalls used by 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 VMware SD-WAN Edge model, including Edge 620 and Edge 3400, logs can be retrieved via the Orchestrator. Alternatively, log events can be sent to an external destination such as a syslog server. For this test cycle, ICSA Labs used logging on both the Orchestrator and the external syslog server.

The following log message depicts how the tested Edge 620 records when a new firewall policy was created from the Orchestrator:

```
11/18/21, 13:36:33  Configuration applied          Edge 620           Info
Applied new configuration for firewall version 1637260527172
```

Initially, ICSA Labs found through testing that Edge 620 and Edge 3400 did not meet all the logging requirements. For details on what was corrected before testing successfully completed, refer to the “Criteria Violations and Resolutions” section of this report.

After VMware addressed the issues reported by ICSA Labs and repairs were subsequently applied and re-tested, the VMware SD-WAN Edges 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 administration-related test cases are aimed, therefore, at ensuring that the firewall requires authentication and that the authentication mechanisms cannot be bypassed. Testing also ensure that remote administration traffic is encrypted.

Results

ICSA Labs remotely administered Edge 620 and Edge 3400 via a VMware-hosted Orchestrator. Attempts to bypass the authentication mechanism for all means of administration were unsuccessful.

Based on the testing results, ICSA Labs determined that Edge 620 and Edge 3400 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

Edge 620 and Edge 3400 continued to maintain their configurations, settings, and data following a forced power outage. Similarly, each of the tested models continued to enforce the configured security policy following the outage.

ICSA Labs determined through testing that Edge 620 and Edge 3400 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 VMware 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 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 testing phases are presented here.

Results

Initially, ICSA Labs discovered that Edge 620 and Edge 3400 did not meet all the functional and security testing requirements. For details, refer to the “Criteria Violations and Resolutions” section of this report.

One behavior ICSA Labs observed while performing reboots of the VMware SD-WAN Edges was the following: For a brief period during a reboot cycle, the tested appliances responded to traffic with ICMP network unreachable messages. Once the firewall completed its reboot cycle, the configured deny rule begins to silently drop the traffic as expected without sending the ICMP unreachable messages.

After VMware addressed the issues reported by ICSA Labs, repairs were subsequently applied and re-tested. Edge 620 and Edge 3400 both met all the functional and security-testing requirements and were not susceptible to attacks (including fragmentation and Denial-of-Service attacks) launched inbound and outbound, to and through the devices. Furthermore, while under attack, the tested VMware SD-WAN Edges continued to permit legitimate traffic according to the security policy.

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

Initially, ICSA Labs found and reported the issues listed below during this test cycle to VMware:

- Did not support FTP bi-directionally between internal and external hosts.
- Did not mitigate the FTP bounce attack.
- Did not mitigate the FTP Fake Client attack (Cert vulnerability 328867).
- Did not properly inspect fragmented packets.
- When preceded by a packet having the SYN flag set, allowed subsequent packets with invalid TCP flag combinations before the destination server responded with a SYN/ACK.
- Acted upon spoofed RST packets with invalid sequence numbers.
- Did not properly mitigate SYN flood attacks in which the attack spoofed the interface IP address of the Edge device.
- Did not properly log NTP/SNTP server availability and time change messages.

VMware subsequently corrected these shortcomings. ICSA Labs then performed re-testing and regression testing. In doing so, ICSA Labs confirmed that the previously reported criteria violations had been remediated and that no new issues were found.

ICSA Labs Certified Firewalls

VMware SD-WAN Edge 620 and Edge 3400 passed all firewall security test cases performed by ICSA labs and met the entire set of baseline and corporate firewall testing criteria requirements. ICSA Labs is pleased to announce that all models in the VMware SD-WAN Edge series have attained 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 over 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

VMware

VMware (NYSE: VMW), a global leader in virtualization and cloud infrastructure, delivers customer-proven solutions that significantly reduce IT complexity and enable more flexible, agile service delivery. VMware accelerates an organization's transition to cloud computing, while preserving existing IT investments and enabling more efficient, agile service delivery without compromising control.

www.vmware.com