Firewall

Certification Testing Report

H3C
H3C SecPath Firewall Family

Tested against these standards
ICSA Labs Firewall Certification Criteria Baseline Module – Version 4.2
ICSA Labs Firewall Certification Criteria Corporate Module – Version 4.2

January 7, 2022

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

Table of Contents

H3C – H3C SecPath Firewall Family
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, the H3C SecPath F1000-AI-80 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 SecPath F1000-AI-80 and the entire SecPath Firewall Family of products retained ICSA Labs Firewall Certification having met all of the testing requirements.

Product Overview

The H3C SecPath Firewall Family is a series of new generation, high-performance firewalls, deployed in small and-medium sized enterprises, LAN network egresses, WAN branches, large-scale enterprise campus networks, service providers, and data centers. The H3C SecPath Firewall Family meets the requirements of Web 2.0 and highly integrates basic and advanced security protections and networking capabilities, including access control, IPS, AV, URL filtering, routing capabilities, IPv4 and IPv6 dual stacks, various VPN services and related protections. High-density GE and 10GE port access capabilities are provided to adapt to all kinds of deployment scenarios. The firewalls adopt H3C's highly-available proprietary software to achieve carrier-level high availability. Redundant power and fan modules help achieve high reliability.

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

H3C provided the following model to ICSA Labs for firewall security certification testing:

- SecPath F1000-AI-80

Software

Testing began with firmware version 7.1.064,Feature 8660P09 and successfully completed with firmware version 7.1.064, Ess 8601P0801.

Documentation

To satisfy documentation requirements, H3C provided ICSA Labs with the following documents in order to assist in the installation, configuration, and administration of their firewall product:

- *H3C Firewall Devices, Fundamentals Configuration 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 SecPath Firewall 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 or series. 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:

F100 Series

F100-C-A1	F100-C-A2

F1000 Series

F1005	F1010	F1090	F1000-AI-05	F1000-AI-10
F1000-AI-15	F1000-AI-25	F1000-AI-35	F1000-AI-55	F1000-AI-60
F1000-AI-65	F1000-AI-70	F1000-AI-75	F1000-AI-80	F1000-AI-90

F5000 Series

F5000-AI-15	F5000-AI-20	F5000-AI-40	F5000-AI160	F5030
F5060	F5080	F5030-D	F5060-D	F5080-D

M9000 Series

M9006	M9010	M9014	M9000-AI-E4	M9000-AI-E8
M9000-AI-E16	M9000-X06	M9000-X10		

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 SecPath F1000-AI-80 in routing mode for both inbound and outbound traffic. In addition to security policy rule changes, ICSA labs made the following configuration change to prepare the SecPath F1000-AI-80 for testing:

- Created custom Firewall Service objects to prevent source Port 0 packets from traversing the firewall:

  ```
  Objects > Object Groups > Service Objects > Create.  When configuring the
  parameters for the service object a select a source port greater than 0.
  ```

- Modified session aging configuration to prevent replayed TCP RST packets from traversing the firewall:

  ```
  [H3C] session aging-time state tcp-close 0.
  ```

- Configured the SecPath to ensure that administrative management access employed crypto with secure ciphers by following the instructions in following documents:

  ```
  H3C Firewall Devices, Fundamentals Configuration Guide

  H3C Firewall Devices, Security Configuration Guide
  ```

- Set IPS to profile to "drop" so that signature 34971 "Fack_FTP_Client_Cert_Vulnerability" would block traffic matching Cert Vulnerability 328867:

  ```
  Objects > IPS > Profiles > Edit ( for active IPS profile)> Action > set to drop.
  ```

- Prevented spoofed traffic by setting uRPF mode to strict:

  ```
  Policies > Attack Defense > IPv4 uRPF > Select Security Zone > Edit > Check mode
  > Strict
  ```

- Created an advanced security policy ACL from the CLI to require Strict TCP session enforcement:

  ```
  [H3C]acl advanced 3000
  [H3C-acl-ipv4-advanced 3000] rule 0 permit tcp syn 1 counting
  [H3C-acl-ipv4-advanced 3000] acl advanced 3001
  [H3C-acl-ipv4-advanced 3001] rule 10 permit ip counting
  [H3C-acl-ipv4-advanced 3001] zone-pair security source <zone> destination <zone>
  [H3C-zone-pair-security-zone-zone]packet-filter 3000
  [H3C-zone-pair-security-zone-zone] packet-filter 3001
  ```

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 SecPath F1000-AI-80 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 SecPath Firewall Family product, including the SecPath F1000-AI-80, logs can be retrieved locally via the web UI and SSH, or log events can be sent to an external server such as a syslog server. For this test cycle, ICSA Labs configured the tested model to send log messages to a private syslog server and to log locally.

The following depicts how the SecPath F1000-AI-80 logs a denied TCP connection attempt:

```
Oct 25 14:21:22 205.160.42.254 2021 H3C %%10FILTER/6/FILTER_ZONE_IPV4_EXECUTION:
SrcZoneName(1025)=Trust;DstZoneName(1035)=Untrust;Type(1067)=ACL;SecurityPolicy(1072)=
Drop;RuleID(1078)=3;Protocol(1001)=TCP;Application(1002)=microsoft-
ds;SrcIPAddr(1003)=205.160.42.66;SrcPort(1004)=0;SrcMacAddr(1021)=aaab-ba00-
0042;DstIPAddr(1007)=205.160.40.66;DstPort(1008)=445;MatchCount(1069)=1;Event(1048)=De
ny;
```

ICSA Labs determined through testing that the SecPath F1000-AI-80 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 SecPath F1000-AI-80 in the lab from the private network using the available web-based GUI via HTTPS and the CLI via SSH. Attempts to bypass the authentication mechanism for all means of administration were unsuccessful.

ICSA Labs determined through testing that the SecPath F1000-AI-80 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 SecPath F1000-AI-80 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 SecPath F1000-AI-80 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 H3C 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

Initially, ICSA Labs discovered that the H3C SecPath F1000-AI-80 did not meet all the functional and security testing requirements. For details, refer to the “Criteria Violations and Resolutions” section of this report.

After H3C addressed the issues reported by ICSA Labs and repairs were subsequently applied, the SecPath Firewall Family met all the functional and security-testing requirements, were not susceptible to attacks launched inbound and outbound to and through the products, including fragmentation and Denial-of-Service attacks. Furthermore, while under attack, the SecPath Firewall Family devices 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

ICSA Labs found and reported the issues listed below during this test cycle. The product initially:

- Did not adequately maintain the state of FTP commands and responses.
- Allowed spoofed TCP reset packets to traverse the firewall.
- Allowed packets with invalid TCP flag combinations when preceded by a SYN before the destination host responded with a SYN/ACK.

H3C corrected these initial shortcomings. ICSA Labs then confirmed through further testing that these issues were indeed resolved.

ICSA Labs Certified Firewalls

Because the SecPath F1000-AI-80 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 SecPath F1000-AI-80 and the other models comprising the H3C SecPath Firewall 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

H3C

H3C is an industry leader in the provisioning of Digital Solutions, and is committed to becoming the most trusted partner of customers in their quest for business innovation and digital transformation. H3C offers a full portfolio of Digital Infrastructure products, spanning across compute, storage, networking, security and related domains, and provides a comprehensive one-stop digital platform that includes cloud computing, big data, interconnectivity, information security, new safety, Internet of Things (IoT), edge computing, artificial intelligence (AI) and 5G solutions, as well as endto-end technical services.

www.h3c.com