ICSA Labs
Network Firewall Certification Testing Report
Corporate – Criteria Version 4.2

A10 Networks, Inc.

Thunder Series Platforms

November 17, 2016

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

FWXX–A10NETWORK-2016-1117-01

Table of Contents

A10 Networks, Inc.
Network Firewall Certification Testing Report
Corporate – Criteria Version 4.2

Executive Summary

Introduction

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For more than 20 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 manages and facilitates technology consortia that focus on emerging, well-defined technologies. The consortia provide for information exchanges among industry leading developers, and for the development of product testing and certification programs and standards. For more information about ICSA Labs, please visit www.icsalabs.com.

Customer Provided Product Overview

The A10 Thunder™ Series is A10 Networks' product family delivering high performance application networking and security solutions, integrating expanded system resources to support future feature needs, and offering our broadest array of physical, virtual and hybrid form factors.

Scope of Assessment

The set of criteria that vendor-submitted products are tested against is an industry-accepted standard to which a consortium of firewall vendors, end users, and ICSA Labs contributed. This standard has evolved over the years into its present iteration – version 4.2 of *The Modular Firewall Certification Criteria.*

During and following initial testing, products remain continuously deployed within this lab environment, which closely approximates the real Internet to ensure more realistic firewall testing. Products are available for and regularly subjected to supplemental testing as new attack techniques emerge and vulnerabilities become known. Only products that continue to meet the criteria under these circumstances retain certification.

Successful firewall product testing culminates in the writing of a report that documents the results of each phase of testing. It also documents the product components submitted by the vendor, any additional configuration used by ICSA Labs to meet the requirements, patches or updates generated during testing, and the mandatory and optional criteria modules against which the product was tested.

Summary of Findings

The Candidate Firewall Product met all the criteria elements in the Baseline and Corporate module and therefore has attained ICSA Labs Firewall Certification. The Candidate Firewall Product will remain continuously deployed at ICSA Labs for the length of the testing contract and will be periodically checked as new attacks and vulnerabilities are discovered. In the event that the Candidate Firewall Product is found susceptible to new attacks or vulnerabilities during a check, ICSA Labs will work with the vendor to resolve the problems in order for the Candidate Firewall Product to maintain its ICSA Labs Firewall Certification.

Certification Maintenance

The Candidate Firewall Product, like all products and product groups that are granted ICSA Labs Firewall Certification, will remain certified on this and future released versions of the product for the length of the testing contract. Future versions will be certified since the product is continuously deployed at ICSA Labs and subjected to periodic spot-checks on the most current product version.

Three circumstances will cause the Candidate Firewall Product to have its ICSA Labs Firewall Certification revoked:

1. The Candidate Firewall Product vendor withdraws from the ICSA Labs Firewall Certification Program.
2. The product fails a periodic spot-check and The Candidate Firewall 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.

Candidate Firewall Product Components

Introduction

The term Candidate Firewall Product or CFP refers to the complete system submitted by the vendor for certification testing including all documentation, hardware, firmware, software, host 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 CFP.

Hardware

- Thunder 4435(S) SPE
- Thunder 5330(S)

Software

Initially, testing began with software version 4.1.0-P2 Build 39. Due to violations reported by ICSA Labs, A10 Networks, Inc. provided updates to address the violations. Testing was successfully completed with 4.1.1-P1 Build 10.

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.
- The functional, integration, and regression testing conducted by the vendor is uniform and consistent across the product family.

Product Family Members

- Thunder 840
- Thunder 930.
- Thunder 1030S
- Thunder 3030S

- Thunder 3230(S)
- Thunder 3430(S)
- Thunder 4430(S)
- Thunder 4440(S)
- Thunder 5330(S)
- Thunder 5430(S)-11
- Thunder 5440(S)
- Thunder 5630(S)
- Thunder 5840(S)
- Thunder 6430(S)
- Thunder 6440(S)
- Thunder 6630(S)
- Thunder 7440(S)
- Thunder 4435(S) SPE
- Thunder 5435(S) SPE.
- Thunder 6435(S) SPE
- Thunder 6635(S) SPE
- Thunder 3030S HVA.
- Thunder 3530S HVA
- VThunder ADC

Documentation

To satisfy documentation requirements, A10 Networks, Inc. provided ICSA Labs with the following documents in order to assist in the installation, configuration, and administration of the CFP:

- *A10 Quick Start Guide 2015*
- *Command Line Interface Reference(3)*
- *System Configuration and Administration Guide*
- *Network Configuration Guide*

Candidate Firewall Product Configuration Tested

Introduction

Firewall products can be configured different ways; therefore, ICSA Labs may face many configuration related decisions before adding a single security policy rule on the CFP. During testing, ICSA Labs attempted to exploit the CFP, so configuration decisions were made to prevent exploitation.

Candidate Firewall Product Configuration

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

The CFP was configured in straight-thru mode for both inbound and outbound connections.

Required Services Security Policy Transition

Introduction

Each phase of CFP testing is performed predominantly while enforcing a particular security policy. Firewall products must be configurable to minimally enforce the security policy 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 service traffic.

Results

ICSA Labs performed port scans followed by additional scans and other tests to ensure that the CFP 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 CFP in either direction.

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

The table below contains a description of the RSSP configuration. The "Traffic Direction" column specifies whether the configured security policy allowed the traffic to enter the private network (Inbound) or the public network (Outbound).

Protocol Port/MsgType	Service Name	Traffic Direction
TCP 21	FTP	Inbound/Outbound
TCP 80	HTTP	Inbound/Outbound
TCP 443	HTTPS	Inbound/Outbound
TCP 25	SMTP	Inbound/Outbound
UDP 53	DNS	Inbound/Outbound
TCP 110	POP3	Inbound/Outbound
TCP 143	IMAP	Inbound/Outbound
TCP 23	Telnet	Outbound

The CFP did not initially meet all of the RSSP requirements. Please see the "Criteria Violations and Resolutions" section for more details about the violation and how it was resolved.

Logging

Introduction

The CFP is required to provide an extensive logging capability. In practice, this degree of logging may not be enabled at all times or by default; however, the capability must exist on CFP in the event that detailed logging is needed.

ICSA Labs tested the logging functionality provided by the CFP ensuring that all permitted and denied traffic was logged for traffic sent both to and through the product. Other events that must be logged are system startups, time changes, access control rule changes, and administrative login attempts. ICSA Labs either configured the local logging mechanism or a remote logging mechanism such as syslog. For all logged events ICSA Labs verified that all required log data were recorded.

Results

The CFP has the ability to store logs on either the product itself or send the logs to a host. The CFP was configured to send log messages to a private host via syslog.

The following log example of a blocked TCP connection to port 22 from a private host to a public host and was taken from syslog.

```
Jul  1 15:18:50 205.160.37.254  Jul  1 02:18:49 2016 ACOS CEF:0|A10
NETWORKS|Thunder Series Unified Application Service Gateway|4.1|102|Session
denied|5|proto=TCP act=Deny rt=4299560551 src=205.160.37.66 spt=5652
dst=205.160.30.66 dpt=22 deviceInboundInterface=ethernet1 cs1=RSSP
cs2=deny_all cs1Label=Policy Name ID cs2Label=Rule Name
```

The CFP met all logging requirements. No violations were found in this area throughout testing.

Administration

Introduction

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 the remote administration traffic was encrypted.

Results

The CFP was remotely administered from a separate management network using the available web-based GUI via HTTPS. Attempts to bypass the authentication mechanism for all means of administration were unsuccessful.

The CFP met all administration requirements. No violations were found in this area throughout testing.

Persistence

Introduction

Power outages, electrical storms, and inadvertent power losses should not cause the CFP 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 CFP against the persistence requirements.

Results

The CFP continued to maintain its configuration, settings, data, and enforcement of the security policy when power was restored following a forced power outage.

The CFP met all persistence requirements. No violations were found in this area throughout testing.

Documentation

Introduction

The CFP documentation should be accurate and applicable to the version tested in providing appropriate guidance for installation, administration, among other information.

Results

ICSA Labs determined the CFP documentation provided adequate and accurate guidance throughout testing for installation and administration.

The CFP met all documentation requirements. No violations were found in this area throughout testing.

Functional and Security Testing

Introduction

Once configured to enforce a security policy the CFP must properly permit the services allowed by that policy. In this case, “properly” means that the service functions correctly. The CFP 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, the product must be configurable for the more secure option. 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 CFP. ICSA Labs used these tools to attempt to defeat or circumvent the security policy enforced by the CFP. Additionally, using trivial Denial-of-Service and fragmentation attacks ICSA Labs attempted to overwhelm or bypass the CFP.

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

Results

The CFP was not susceptible to attacks launched inbound and outbound to and through the CFP, including fragmentation and trivial Denial-of-Service attacks, while properly providing the required functional services.

The CFP did not initially meet all of the functional and security requirements. Please see the “Criteria Violations and Resolutions” section for more details about the violation and how it was resolved.

Notes

During testing, it was noted that the product allowed TCP RST’s to be replayed for 10 seconds, while not a violation, A10 Networks elected to resolve this with the certified firmware version.

Criteria Violations and Resolutions

Introduction

In the event that ICSA Labs uncovers criteria violations while testing the CFP, the vendor must make repairs before testing can be completed and certification granted. The section that follows documents all criteria violations discovered during testing.

Results

The following criteria violations were found by ICSA Labs during testing. Updates were submitted by A10 Networks, Inc. to address the violations which were then successfully tested:

- The CFP allowed TCP traffic through the CFP without first establishing a proper TCP connection. After receiving a SYN-ACK from the server the CFP allowed unauthorized traffic from the client.
- The CFP was susceptible to an evasion technique enabling an FTP bounce attack.

Testing Information

This report is issued by the authority of the Managing Director, ICSA Labs. Tests are done under normal operating conditions.

Lab Report Date

November 17, 2016

Please visit www.icsalabs.com for the most current information about this and other products.

Test Location

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

Product Developer's Headquarters

A10 Networks, Inc.
3 West Plumeria Drive
San Jose, CA 95134

This test is accredited under ICSA Labs' ISO/IEC 17025 accreditation issued by ANSI-ASQ National Accreditation Board. Refer to certificate and scope of accreditation number AT – 1423.