ICSA labs
An Independent Division
of Verizon

ICSA Labs
Firewall Certification Criteria
Baseline Module - Version 4.2

Document Version 1.1
September 1, 2016

www.icsalabs.com

Firewall Certification Criteria
Baseline Module - Version 4.2

Table of Contents

Module Overview

The Modular Firewall Certification Criteria is aimed at firewall products that filter *traffic* in TCP/IP networks. The ICSA Labs Firewall Certification Program does not test and certify products that filter *traffic* in IPX, SNA, AppleTalk and other non-TCP/IP network architectures.

In addition to this module, there are four Required Services *Security Policy* criteria modules – Residential, Small/Medium Business (SMB), Corporate and Enterprise. Vendors must formally select one of the four prior to submitting a *Candidate Firewall Product* for testing. Each Required Services *Security Policy* criteria module targets one of the following broad market segments: consumers, telecommuters, general-purpose firewalls and enterprise level firewall purchasers. To attain ICSA Labs Firewall Certification, the *Candidate Firewall Product* must completely satisfy all functional and assurance requirements in this Baseline module and all requirements in the chosen Required Services *Security Policy* criteria module.

Though it is not mandatory, vendors may formally elect to have their product tested against an additional module(s), when such modules are appropriate. These optional modules are completely independent from one another as well as from the Baseline and Required Services *Security Policy* modules. To claim ICSA Labs Firewall Certification in conjunction with an additional, optional module(s) *Candidate Firewall Product*s must completely satisfy all requirements in the selected module(s).

With the exception of the Documentation requirements, and unless otherwise noted, the *Candidate Firewall Product* must only meet the requirements that appear in this and the other modules after having been installed and configured according to the Installation Documentation (reference DO1 in this document). The Documentation requirements must be met at all times before and after installation.

Refer to the Glossary for a definition of terms used in this and all module documents. Any words italicized within this document will be found in the Glossary.

Required Services Security Policy

RS1 – Required Services Security Policy

Satisfying the Required Services *Security Policy* Module – The *Candidate Firewall Product* must completely satisfy all requirements in the distinct Required Services *Security Policy* module selected by the *Candidate Firewall Product* vendor prior to testing.

NOTE1 TO RS1 -- Throughout the remainder of this module the term "*security policy*" refers to the set(s) of permitted and denied services in the vendor-chosen Required Services *Security Policy* module or the applicable areas in selected Optional Modules.

Logging

LO1 – Required Events

The *Candidate Firewall Product* (CFP) must have the capability, though it does not have to be enabled by default, to *log* the following event types:

A. All permitted inbound access requests from public network clients that use a service identified in the *security policy* hosted on the CFP itself or on a private or service network server;
B. All permitted outbound *access request*s from private and service network clients that use a service identified in the *security policy* on a public network server;
C. All *drop*ped or denied *access request*s from private, service and public network clients to traverse the CFP that violate the *security policy* (see NOTE2 TO LO1);
D. All *drop*ped or denied *access request*s from private, service and public network clients to send *traffic* to the CFP itself that violate the *security policy* (see NOTE2 TO LO1);
E. All attempts to *authenticate* at an *Administrative Interface* (see AD2 in this document) on the CFP itself;
F. All *access request*s from private, service and public network clients to send *traffic* to the CFP itself on the port or ports used for *Remote Administration* (see the *Remote Administration* requirements in the applicable RSSP document);
G. Each startup; of the system itself or the of the *security policy* enforcement component(s);
H. All manually entered changes to the system clock.

NOTE1 TO LO1 – There is no requirement that the CFP *log* at all times or that it *log* by default. In fact, the CFP may have individual mechanisms for enabling and disabling *logging* for each of the above events as well as for each of the Required *Log* Events that appear in other modules.

NOTE2 TO LO1 - *Logging* of *drop*ped *traffic* is not required provided that it is not possible to configure the CFP to allow said *traffic* or when the CFP is *drop*ping the *traffic* in response to a dynamic condition, such as a detected flood attack. In either case, this behavior must be documented as per DO6 below.

NOTE1 TO LO1, E – *Logging* of both successful and failed authentication attempts is required only for *Administrative Interface*s which are necessary for meeting one or more criteria requirements or for *Administrative Interface*s which cannot be disabled. Local *Administrative Interface*s not necessary for meeting criteria requirements can be considered disabled through physical means.

NOTE1 TO LO1, G – In the event that multiple software components are installed on the *security policy* enforcement hardware, then the CFP may *log* startup of any or all of these software components, that may include but are not limited to the operating system and the *security policy* enforcement software itself, in order to satisfy the requirement.

NOTE1 TO LO1, H – This requirement is not applicable to CFPs being tested against the Enterprise Module Firewall Certification Criteria.

LO2 – Required Data

For each Required *Log* Event, the following *log* data elements must, when applicable, be accurately *captured* in a *log*:

A. Date and Time – when the event occurred;
   1. The date recorded by the CFP for each event in the *log* must consist of the four-digit year, the month and the day of the month.
   2. The time recorded by the CFP for each event in the *log* must consist of the hour, the minute and the second.
B. Protocol – indicated in the IP header field;
C. Source IP Address – from the CFP’s perspective;
D. Destination IP Address – from the CFP’s perspective;
E. Source Port (TCP and UDP);
F. Destination Port (TCP and UDP);
G. Message Type (ICMP);

H. Disposition of the Event (see DO5 in this document);
I. Statement of success or failure to *authenticate* at an *Administrative Interface* (see AD2 in this document);
    1. Failed authentication attempts must include the reason for the failure.

NOTE1 TO LO2 – In the event that multiple components comprise the CFP, it is perfectly acceptable that one of the components captures *traffic*-related *log* data while another component captures authentication-related *log* data.

NOTE2 TO LO2 – In accordance with the LO1,H requirement to *log* system clock change events, the date and time both before and after the change must be recorded using the data elements required by LO2,A.

NOTE1 TO LO2,A – Any date formatting that is outlined in ISO 8601:2004 (Representation of Dates and Times) will be acceptable provided required data is present.

LO3 – Precision of Date and Time

The date and time recorded in the *log* by the *Candidate Firewall Product* for Required *Log* Events must reflect the exact date and must minimally reflect the exact second in time that the event occurred.

LO4 – Data Presentation

All Required *Log* Data corresponding to all Required *Log* Events must be available for review upon demand and presented in a human readable format while preserving the relative sequence of events.

LO5 (Conditional) – Logs Sent To Separate Candidate Firewall Component

In the event that Required *Log* Data is sent from one *Candidate Firewall Product* component to a separate *Candidate Firewall Product* component, then some unique identifier of the *Candidate Firewall Product* component point of origin marking each individual Required *Log* Event must be included with the data sent to the separate *Candidate Firewall Product* component.

LO6 (Conditional) – Linking Multiple *Log*s for a Single Event

In the event that the CFP uses multiple *log*s as repositories for elements of Required *Log* Data related to a single Required *Log* Event, then some clear, accurate correlation between the elements in each of the multiple *log*s must exist linking them together to the appropriate event.

Administration

AD1 – Administrative Functions

Administrative Functions must exist as part of the *Candidate Firewall Product* to:

A. Configure and change or acquire the date and time;
B. Configure and change *Authentication Configuration Data*;
C. Configure and change *Remote Administration* settings;
D. Enable *logging* of the Required *Log* Events;
E. Review Required *Log* Data.

NOTE1 TO AD1,A – In the event that a product supports time and date acquisition, the related *administrative functions* must include an option to disable time and date acquisition.

NOTE1 TO AD1,C – Refer to the appropriate *Remote Administration* section of the chosen Required Services *Security Policy* (RSSP) module as the specific requirement for *Remote Administration* will vary.

AD2 – Administrative Interface

The *Candidate Firewall Product* must include an *Administrative Interface* from which the *Candidate Firewall Product Administrative Functions* are accessible.

NOTE1 TO AD2 – Refer to AD6 in SMB, Corporate or Enterprise Required Services *Security Policy* (RSSP) modules.

AD3 – Administrative Interface Authentication

To access the *Administrative Functions* via the *Administrative Interface*, the *Candidate Firewall Product* must have the capability to require authentication through the *Administrative Interface* using an Authentication Mechanism.

NOTE1 TO AD3 – The "capability to require authentication" must exist on all *Candidate Firewall Product*s regardless of the chosen Required Services *Security Policy* module. However, only the Required Services *Security Policy* SMB, Corporate and Enterprise modules explicitly specify the Authentication Mechanism to use. Since no Authentication Mechanism requirement appears in the Required Services *Security Policy* Residential module, it is acceptable for the Authentication Mechanism to be disabled and/or to set the *Authentication Configuration Data* to NULL (or similar).

Persistence

PE1 – Security Policy

When electrical power is reapplied after being lost or removed from the *Candidate Firewall Product*, the *Candidate Firewall Product* must do one of the following:

A. Enforce the same *security policy* that was being enforced prior to the loss or removal of power; or
B. Enforce a *deny*-all *security policy*, while including an Administrative Function(s) capable of restoring the *Candidate Firewall Product* to the same *security policy* that was being enforced prior to the loss or removal of power.

PE2 – Logs

In the event that electrical power is lost or removed from the *Candidate Firewall Product*, all Required *Log* Data for all Required *Log* Events not in transit between *Candidate Firewall Product* components must persist and remain the same when electrical power is reapplied.

PE3 – Authentication Configuration Data

In the event that electrical power is lost or removed from the *Candidate Firewall Product*, all *Authentication Configuration Data* (refer to AD1,B in this document) must persist and remain the same when electrical power is reapplied.

PE4 – Remote Administration Configuration

In the event that electrical power is lost or removed from the *Candidate Firewall Product*, *Remote Administration* settings must remain configured the same when electrical power is reapplied.

NOTE1 TO PERSISTENCE REQUIREMENTS – The PERSISTENCE requirements are not intended to cover situations where electrical power is lost or removed while exercising any of the *Administrative Functions*.

NOTE2 TO PERSISTENCE REQUIREMENTS – With the exception of PE1, the PERSISTENCE requirements are not intended to cover situations where the *Candidate Firewall Product* hardware becomes faulty as a result of a loss or removal of power.

Functional Testing

FT1 – Services Tested

Testing the *Candidate Firewall Product* while enforcing a *security policy* must demonstrate that the services in that *security policy* pass through the *Candidate Firewall Product* properly and that no other services can be passed through the *Candidate Firewall Product* that are not explicitly enabled in that *security policy*.

NOTE1 TO FT1 – For each valid *access request* passed through the *Candidate Firewall Product* that elicits a response either after arriving at the destination host or while en route to the destination host, the *Candidate Firewall Product* may pass back to the client no more than a single, directly-related response.

Barring compelling indications or references describing a case where a multiple IP datagram "response" legitimately occurs, a "response" is no more than a single IP datagram.

FT2 – Administrative Functions

The *Candidate Firewall Product* must demonstrate through testing that its *Administrative Functions* (refer to AD1 in this document) work properly.

Security Testing

ST1 – Administrative Access

The *Candidate Firewall Product* must demonstrate through testing that no unauthorized control of its *Administrative Functions* (refer to AD1 in this document) can be obtained.

ST2 – Vulnerabilities

When enforcing a *security policy*, the *Candidate Firewall Product* must demonstrate through testing that it is not vulnerable to the evolving set of vulnerabilities known in the Internet community that are capable of being remotely tested.

ST3 – No Vulnerabilities Introduced

When enforcing a *security policy*, the *Candidate Firewall Product* must demonstrate through testing that it does not introduce vulnerabilities to private and service network servers.

ST4 – No Other Traffic

The *Candidate Firewall Product* must demonstrate through testing that nothing other than that specified in the *security policy* traverses the *Candidate Firewall Product*.

ST5 – Denial of Service

The *Candidate Firewall Product* must demonstrate through testing that:

A. It is not rendered inoperable by any *trivial denial of service* type attacks; and
B. It fails closed if rendered inoperable through any denial of service type attack for which there is no known defense.

ST6 – Fragmented Packets

The *Candidate Firewall Product* must demonstrate through testing that fragmented packets can be denied from traversing the *Candidate Firewall Product*.

NOTE1 TO ST6 – For all services including the set of Required Services, the *Candidate Firewall Product* (CFP) must have the capability, though it need not be the default CFP behavior, to either:

a) *drop* IP datagram fragments arriving at a CFP interface, or

b) correctly reassemble fragmented IP datagrams on the CFP and pass the reassembled IP datagrams toward their destination as long as they do not violate the *security policy* being enforced on the CFP.

NOTE2 TO ST6 – It is acceptable for *Candidate Firewall Product*s to receive fragmented IP datagrams that meet the *security policy*, correctly reassemble them, and then fragment the resulting IP datagrams prior to sending them out. However, this is only permissible when warranted by the MTU of the next closest network segment to the destination.

Documentation

DO1 – Installation

The *Candidate Firewall Product* must include some measure of written and/or electronic guidance indicating how to properly install the *Candidate Firewall Product*.

DO2 – Administration

The *Candidate Firewall Product* must include all written and/or electronic guidance applicable for administering and maintaining the product.

DO3 – Additional Documents

The written and/or electronic *Candidate Firewall Product* documentation must indicate:

A. The minimum hardware requirements for all components of the *Candidate Firewall Product*;
B. The base version of all software and firmware components comprising the *Candidate Firewall Product*;
C. Whether or not customer support is available;
D. CONDITIONAL – Where and how customers access customer support, in the event that customer support is available;
E. CONDITIONAL – Where to obtain patches and how to apply them in the event that patches are required for any component of the *Candidate Firewall Product*.

DO4 – Accurate

All *Candidate Firewall Product* documentation used for the purposes of testing may not be inaccurate.

DO5 – Log Event Dispositions

The *Candidate Firewall Product* must include written and/or electronic guidance defining all possible values that indicate a Disposition of the Event (refer to LO2,H in this document).

DO6 (Conditional) – Logging Exceptions

In the event that the *Candidate Firewall Product* (CFP) *drop*s certain types of *traffic* without *logging* it, the CFP must include written and/or electronic guidance describing the *traffic* and the circumstances under which the *traffic* is *drop*ped without being *logged*.