

1 Modular Firewall Certification Criteria 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.

There are three Required Services Security Policy modules. Vendors must formally select one of the three prior to submitting a Candidate Firewall Product for testing. Each Required Services Security Policy module targets one of the following broad market segments: consumers, telecommuters, and general-purpose 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 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 Products 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.ⁱ 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.

2 Module Requirements

REQUIRED SERVICES SECURITY POLICY

RS1 – 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.ⁱⁱ

LOGGING

LO1 – Required Log Events – The Candidate Firewall Product 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 Candidate Firewall Product itself or on a private or service network server;
- B. All permitted outbound access requests from private and service network clients that use a service identified in the security policy on a public network server;
- C. All access requests from private, service and public network clients to traverse the Candidate Firewall Product that violate the security policy;
- D. All access requests from private, service and public network clients to send traffic to the Candidate Firewall Product itself that violate the security policy;
- E. All attempts to authenticate at an Administrative Interfaceⁱⁱⁱ on the Candidate Firewall Product itself;
- F. All access requests from private, service and public network clients to send traffic to the Candidate Firewall Product itself on the port or ports used for Remote Administration^{iv};
- 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 Candidate Firewall Product log at all times or that it log by default. In fact, the Candidate Firewall Product 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^v.

NOTE1 TO LO1, E – With respect to a Candidate Firewall Product (CFP) tested against the Residential or SMB Required Services Security Policy modules, unless a remote administration administrative interface is enabled by default, or enabled during testing to meet one or more criteria requirements, then logging of both successful and failed authentication attempts from that interface is not required. Successful and failed authentication attempts from at least one remote administration administrative interface must be logged properly whether or not it is enabled by default.

NOTE2 TO LO1, E – With respect to a Candidate Firewall Product (CFP) tested against the Corporate Required Services Security Policy module, unless a remote/local administration administrative interface is enabled by default, or enabled during testing to meet one or more criteria requirements, then logging of both successful and failed authentication attempts from that interface is not required. Successful and failed authentication attempts from at least one remote and one local administration administrative interface must be logged properly whether or not they are enabled by default.

NOTE1 TO LO1, G – In the event that multiple software components are installed on the security policy enforcement hardware, then the Candidate Firewall Product (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.

LO2 – Required Log Data – For each Required Log Event^{vi}, 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 Candidate Firewall Product for each event in the log must consist of the four-digit year, the month and the date.
 - 2. The time recorded by the Candidate Firewall Product 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 Candidate Firewall Product's perspective;
- D. Destination IP Address – from the Candidate Firewall Product's perspective;
- E. Source Port (TCP and UDP);
- F. Destination Port (TCP and UDP);
- G. Message Type (ICMP);
- H. Disposition of the Event^{vii};
- I. Statement of success or failure to authenticate at an Administrative Interface^{viii};
 - 1. Failed authentication attempts must include the reason for the failure.

NOTE1 TO LO2 – In the event that multiple components comprise the Candidate Firewall Product, it is perfectly acceptable that the one of the components captures packet-related log data elements 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.

LO3 – Precision of Date and Time – The date and time recorded in the log by the Candidate Firewall Product for Required Log Events^{ix} must reflect the exact date and must minimally reflect the exact second in time that the event occurred.

LO4 – Log Data Presentation – All Required Log Data^x corresponding to all Required Log Events^{xi} must be available for review upon demand and presented in a human readable format while preserving the relative sequence of events.

CONDITIONAL – LO5 – Logs Sent to Separate Candidate Firewall Product Component – In the event that Required Log Data^{xii} 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^{xiii} must be included with the data sent to the separate Candidate Firewall Product component.

CONDITIONAL – LO6 – Linking Multiple Logs for a Single Event – In the event that the Candidate Firewall Product uses multiple logs as repositories for elements of Required Log Data^{xiv} related to a single Required Log Event^{xv}, then some clear, accurate correlation between the elements in each of the multiple logs 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^{xvi} settings;
- D. Enable logging of the Required Log Events^{xvii};
- E. Review Required Log Data^{xviii}.

AD2 – Administrative Interface – The Candidate Firewall Product must include an Administrative Interface from which the Candidate Firewall Product Administrative Functions^{xix} are accessible.

AD3 – Administrative Interface Authentication – To access the Administrative Functions^{xx}, the Candidate Firewall Product must have the capability to require authentication through an Administrative Interface^{xxi} using an Authentication Mechanism^{xxii}.

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 AD3 – The “capability to require authentication” must exist on all Candidate Firewall Products regardless of the chosen Required Services Security Policy module. However, only the Required Services Security Policy SMB & Corporate modules explicitly specify the Authentication Mechanism^{xxiii} to use. Since no Authentication Mechanism^{xxiv} requirement appears in the Required Services Security Policy Residential module, it is acceptable for the Authentication Mechanism^{xxv} to be disabled and/or to set the Authentication Configuration Data^{xxvi} to NULL (or similar).

PERSISTENCE

PE1 – Security Policy Persistence – 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 – Log Persistence – In the event that electrical power is lost or removed from the Candidate Firewall Product, all Required Log Data^{xxvii} for all Required Log Events^{xxviii} not in transit between Candidate Firewall Product components must persist and remain the same when electrical power is reapplied.

PE3 – Authentication Configuration Data Persistence – In the event that electrical power is lost or removed from the Candidate Firewall Product, all Authentication Configuration Data^{xxix} must persist and remain the same when electrical power is reapplied.

PE4 – Remote Administration Configuration Persistence – In the event that electrical power is lost or removed from the Candidate Firewall Product, Remote Administration^{xxx} 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^{xxxi}.

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 Testing – 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 Testing – The Candidate Firewall Product must demonstrate through testing that its Administrative Functions^{xxxii} work properly.

SECURITY TESTING

ST1 – Administrative Access Testing – The Candidate Firewall Product must demonstrate through testing that no unauthorized control of its Administrative Functions^{xxxiii} can be obtained.

ST2 – Vulnerability Testing – 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 Products 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 Documentation – 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 Documentation – The Candidate Firewall Product must include all written and/or electronic guidance applicable for administering and maintaining the product.

DO3 – Additional Documented Coverage – 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 Documentation – All Candidate Firewall Product documentation used for the purposes of testing may not be inaccurate.

DO5 – Log Event Dispositions Defined – The Candidate Firewall Product must include written and/or electronic guidance defining all possible values that indicate a Disposition of the Event^{xxxiv}.

ⁱ Refer to DO1 in this module.

ⁱⁱ This is applicable only in the event that the Candidate Firewall Product is also being tested against the Extended Services module

ⁱⁱⁱ Refer to AD2 in this module.

-
- iv Depending on which Required Services Security Policy module was chosen by the vendor prior to testing, refer to either AD4 in the Required Services Security Policy - Residential module, AD7 in the Required Services Security Policy - SMB module, or AD8 in the Required Services Security Policy - Corporate module.
 - v For other modules that contain Required Log Events refer to LO7 in the Required Services Security Policy - Corporate module and to LO8 in the Management module.
 - vi Refer to LO1 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and LO8 in the Management module.
 - vii Refer to DO5 in this module.
 - viii Refer to AD2 in this module.
 - ix Refer to LO1 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and LO8 in the Management module.
 - x Refer to LO2, LO5 and LO6 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and to LO8 in the Management module.
 - xi Refer to LO1 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and LO8 in the Management module.
 - xii Refer to LO2, LO5 and LO6 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and to LO8 in the Management module.
 - xiii Refer to LO1 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and LO8 in the Management module.
 - xiv Refer to LO2, LO5 and LO6 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and to LO8 in the Management module.
 - xv Refer to LO1 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and LO8 in the Management module.
 - xvi Depending on which Required Services Security Policy module was chosen by the vendor prior to testing, refer to either AD4 in the Required Services Security Policy - Residential module, AD7 in the Required Services Security Policy - SMB module, or AD8 in the Required Services Security Policy - Corporate module.
 - xvii Refer to LO1 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and LO8 in the Management module.
 - xviii Refer to LO2, LO5 and LO6 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and to LO8 in the Management module.
 - xix Refer to AD1 in this module and, if applicable, to PE1,B in this module, AD6 in the Required Services Security Policy - SMB or Corporate modules and AD8 in the Management module.
 - xx Refer to AD1 in this module and, if applicable, to PE1,B in this module, AD6 in the Required Services Security Policy - SMB or Corporate modules and AD8 in the Management module.
 - xxi Refer to AD2 in this module.
 - xxii There is no Authentication Mechanism requirement in Required Services Security Policy - Residential module. If applicable, refer to AD5 in the Required Services Security Policy - SMB or Corporate modules.
 - xxiii If applicable, refer to AD5 in the Required Services Security Policy - SMB or Corporate modules. There is no Authentication Mechanism requirement in the Required Services Security Policy - Residential module.
 - xxiv If applicable, refer to AD5 in the Required Services Security Policy - SMB or Corporate modules. There is no Authentication Mechanism requirement in the Required Services Security Policy - Residential module.
 - xxv There is no Authentication Mechanism requirement in the Required Services Security Policy - Residential module. If applicable, refer to AD5 in the Required Services Security Policy - SMB or Corporate modules.
 - xxvi Refer to AD1,B in this module.
 - xxvii Refer to LO2, LO5 and LO6 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and to LO8 in the Management module.
 - xxviii Refer to LO1 in this module and, if applicable, to LO7 in the Required Services Security Policy - Corporate module and LO8 in the Management module.
 - xxix Refer to AD1,B in this module.
 - xxx Depending on which Required Services Security Policy module was chosen by the vendor prior to testing, refer to either AD4 in the Required Services Security Policy - Residential module, AD7 in the Required Services Security Policy - SMB module, or AD8 in the Required Services Security Policy - Corporate module.
 - xxxii Refer to AD1 in this module and, if applicable, to PE1,B in this module, AD6 in the Required Services Security Policy - SMB or Corporate modules and AD8 in the Management module.

-
- xxxii Refer to AD1 in this module and, if applicable, to PE1,B in this module, AD6 in the Required Services Security Policy - SMB or Corporate modules and AD8 in the Management module.
- xxxiii Refer to AD1 in this module and, if applicable, to PE1,B in this module, AD6 in the Required Services Security Policy - SMB or Corporate modules and AD8 in the Management module.
- xxxiv Refer to LO2,H in this module.