

A. 4.1a Logging Update Overview

This document updates the Logging Criteria contained in version 4.1 of the Modular Firewall Certification Criteria Baseline module. Updated Glossary Definitions are included as well. Products successfully tested against the updated Logging Criteria will receive a 4.1a ICSA Labs Firewall Certification.

This updated Logging Criteria has been introduced to address two specific issues:

1. Products which drop certain types of traffic without the ability to log the dropped traffic. Under the 4.1 Criteria, this is not acceptable. Under the updated 4.1a Criteria, this will be acceptable in certain circumstances.
2. Products which can only meet the 4.1 Criteria if debug output captured via an administrative interface is considered a form of logging. This was not intended to be acceptable under the 4.1 Criteria. The updated 4.1a Criteria clarifies that this is not acceptable.

This update does not affect any products which have been successfully tested against the 4.1 Criteria. Therefore, products with an existing 4.1 ICSA Labs Firewall Certification will maintain their certified status without the need for testing against the updated criteria. There is no difference in status between 4.1 and 4.1a certifications.

B. Updated 4.1a Logging Criteria

The following **LOGGING** section replaces the **LOGGING** section found in the version 4.1 of the Modular Firewall Certification Criteria Baseline module.

LOGGING

LO1 – Required Log 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 requests from private and service network clients that use a service identified in the security policy on a public network server;
- C. All dropped or denied access requests from private, service and public network clients to traverse the CFP that violate the security policy (see NOTE2 TO LO1);
- D. All dropped or denied access requests 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 on the CFP itself;
- F. All access requests from private, service and public network clients to send traffic to the CFP itself on the port or ports used for Remote Administration;
- 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 dropped traffic is not required provided that it is not possible to configure the CFP to allow said traffic or when the CFP is dropping 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 Interfaces which are necessary for meeting one or more criteria requirements or for Administrative Interfaces which cannot be disabled. Local Administrative Interfaces 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.

LO2 – Required Log 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 date.
 - 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;
- I. Statement of success or failure to authenticate at an Administrative Interface;
 - 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.

LO3 – Precision of Date and Time – The date and time recorded in the log by the CFP for Required Log Events 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 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.

CONDITIONAL – LO5 – Logs Sent to Separate Candidate Firewall Component – In the event that Required Log Data is sent from one CFP component to a separate CFP component, then some

unique identifier of the CFP component point of origin marking each individual Required Log Event must be included with the data sent to the separate CFP component.

CONDITIONAL – LO6 – Linking Multiple Logs for a Single Event – In the event that the CFP uses multiple logs 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 logs must exist linking them together to the appropriate event.

The following **DOCUMENTATION** requirement is in addition to those found in version 4.1 of the Modular Firewall Certification Criteria Baseline module.

DOCUMENTATION

CONDITIONAL – DO6 – Logging Exceptions Defined – In the event that the Candidate Firewall Product (CFP) drops 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 dropped without being logged.

C. Updated 4.1a Glossary Definitions

The following definitions replace those found in version 4.1 of the Modular Firewall Certification Criteria Glossary.

Access Request – The term *access request* refers to any instance where *traffic* arriving on a network segment corresponding to one of the *Candidate Firewall Products'* network interfaces is compared against the access control rules or another non-connection-related, access control structure (e.g., an IP spoofing-related structure) on the *Candidate Firewall Product*.

An *access request* would not include passing *traffic* through the *Candidate Firewall Product* where that *traffic* is part of an ongoing connection. Though many TCP packets may be associated with a session, only one of those packets represents the *access request*. Even though UDP is session-less, vendors often create state using a timer or other mechanism. Thus for all UDP packets belonging to a UDP “session” (i.e., before the timer expires) only one of those packets represents the actual *access request*. The rest are part of the UDP “session”.

The implication of the *access request* term for the logging requirements in the criteria is that only a single entry needs to be recorded for TCP sessions and UDP “sessions”. However, for *traffic* which does not belong to a TCP session or UDP “session” as well as for ICMP and other *traffic* violating the *security policy*, the *Candidate Firewall Product* must *log* every packet when such *logging* is enabled.

Log – When it appears as a noun, it refers to a non-volatile physical storage space on some component of the *Candidate Firewall Product* including a dedicated separate logging server where log data elements are permanently stored in a record-oriented format (unless they are deleted by an administrator). A *log* may not be overwritten by default. Log Data sent to and received by a user via email is considered an alert and does not constitute a *Log*. Log Data sent as streaming output to a console port or another administrative interface is considered debugging information and does not constitute a *Log*.

Security Policy – This is a high-level description of the handling of *services* explicitly permitted and/or denied to or through the *Candidate Firewall Product*. This includes all actions the product takes in response to network *traffic*, such as but not limited to *Drop*, *Deny*, and *Logging*. Each

Required Services Security Policy module has a *security policy* that must be enforced by the *Candidate Firewall Product* upon installation.

The following definitions are in addition to those found in version 4.1 of the Modular Firewall Certification Criteria Glossary.

Logged, Logging, or Log when it appears as a verb – This term refers to both recording and then storing elements of data by the *Candidate Firewall Product* in a *Log*. Synonymous with *Captured*.

Traffic – The Modular Firewall Certification Criteria is aimed at firewall products that filter *traffic* in TCP/IP networks. Therefore, products are not required to handle non-TCP/IP *traffic* such as IPX, SNA, AppleTalk and other non-TCP/IP network architectures. Thus, non-TCP/IP *traffic* may be ignored and logging of such *traffic* is not required. Firewall products may handle Address Resolution Protocol (ARP) *traffic* in order for TCP/IP to function, however logging of ARP *traffic* is also not required.