

1 Module Overview

This module is targeted at vendor firewall products designed to serve as general-purpose firewalls. It is also the module that, in conjunction with the Baseline module, most closely represents the evolution of the Firewall Product Certification Criteria.

Vendor firewall products satisfying the requirements in this module will have to enforce, upon proper installation, a default security policy denying all inbound non-Remote Administration related traffic originating from public network sources. Later, the product will have to be configured to enforce another security policy allowing a standard set of services inbound and outbound. Therefore, a means to configure Access Control Rules will be available on the product. Also, the product will include the capability for administration over an encrypted link as well as functionality to locally administer the product. Both means of administration require authentication before access to administrative functions is granted. The product will log the occurrence of changes to the Access Control Rules and the date and time will persist in the event that there is a loss or removal of power. Finally, the product can be properly configured and will enforce a specific security policy regardless of the documented mode used to configure that security policy.

2 Module Requirements

REQUIRED SERVICES SECURITY POLICY - CORPORATE CATEGORY

RSC1 – Enforcing the Default Security Policy – After being installed according to the Installation Documentation,ⁱ the Candidate Firewall Product must immediately enforce the Default Security Policy as defined below:

- A. Traffic Denied Inbound – The Candidate Firewall Product must drop or deny non-Remote Administrationⁱⁱ related access requests from public network clients directed to:
 - 1. Private network hosts;
 - 2. Service network hosts;
 - 3. The Candidate Firewall Product itself.

NOTE1 TO RSC1 – A complete deny-all inbound policy is an acceptable way to meet RSC1. There are no restrictions on the default services permitted and denied outbound.

NOTE2 TO RSC1 – It shall be permissible for the Candidate Firewall Product to send and receive traffic related to acquiring the current time and date.

RSC2 – Enforcing the Required Services Security Policy – After configuring Access Control Rules,ⁱⁱⁱ the Candidate Firewall Product must enforce the Required Services Security Policy as defined below:

- A. Traffic Permitted Inbound – The Candidate Firewall Product must support access requests from public network clients to services on private and service network servers that must exist independent of the Candidate Firewall Product. Such requests must be permitted for the following services:
 - 1. FTP (Active and Passive Mode)
 - 2. HTTP
 - 3. HTTPS
 - 4. SMTP
 - 5. DNS (may be hosted by the firewall)
 - 6. POP3
 - 7. IMAP
- B. Traffic Permitted Outbound – The Candidate Firewall Product must support access requests from private and service network clients to services on public network servers. Such requests must be permitted for the following services:

ICSA Labs

The Modular Firewall Certification Criteria



Required Services Security Policy - Corporate Category module - version 4.1

1. TELNET
2. FTP (Active and Passive Mode)
3. HTTP
4. HTTPS
5. SMTP
6. DNS
7. POP3
8. IMAP

- C. Traffic Permitted for Candidate Firewall Product -- The Candidate Firewall Product may permit access requests for the following services:
1. Remote Administration^{iv} access requests from private, service and public network clients to the Candidate Firewall Product
 2. Time and date acquisition access requests from the Candidate Firewall Product to private, service and public network servers
- D. All other traffic from both private, service and public network clients directed to or through the Candidate Firewall Product must be dropped or denied.

NOTE1 TO RSC2 – It is acceptable for Candidate Firewall Products to require that one or more of the servers hosting required services in RSC2,A be located on the service network.

NOTE2 TO RSC2,B & C – The Candidate Firewall Product may require that private and service network clients use SOCKS4 or SOCKS5 to satisfy RSC2,B. Therefore, in such cases, it is permissible for a single standard or non-standard port to be open on the Candidate Firewall Product for the SOCKS Server that will not drop or deny packets.

NOTE3 TO RSC2,D – RSC2,D is true unless the Candidate Firewall Product is being tested against the Extended Services module, in which case there are some additional services permitted inbound and outbound presented in that module.

RSC3 – No Special Software or Specific Platforms – With the exception of management station hosts, the Candidate Firewall Product must not require the introduction or installation of proprietary or otherwise special, non-SOCKS related software on private, service and public network hosts. Also with the exception of management station hosts, the Candidate Firewall Product must neither require a specific platform or operating system, nor specifically exclude support for any platform or operating system, on private, service and public network hosts.

ADMINISTRATION

AD5 – Authentication Mechanism – A valid password or some stronger Authentication Mechanism must be used before access to Administrative Functions^v is granted.

AD6 – Access Control Rules Administrative Functions – Administrative Functions must exist on the Candidate Firewall Product to:

- A. Create Access Control Rules that properly:
1. Implement the Required Services Security Policy^{vi};
 2. Enforce a security policy different than the Default Security Policy and the Required Services Security Policy that properly permits service traffic, originating from network clients and destined for the network servers, through the Candidate Firewall Product while dropping or denying all other traffic.
- B. Review the Access Control Rules.

ICSA Labs

The Modular Firewall Certification Criteria



Required Services Security Policy - Corporate Category module - version 4.1

C. Alter the Access Control Rules.

AD8 – Remote Administration – The Candidate Firewall Product must permit Remote Administration having the following characteristic in addition to that of AD5^{vii}:

A. The Remote Administration traffic must be encrypted;

AD9 – Local Administration – The Candidate Firewall Product must permit Local Administration through an Administrative Interface^{viii} in accordance with AD5^{ix}.

PERSISTENCE

PE5 – Date and Time Persistence – In the event that electrical power is lost or removed from the Candidate Firewall Product, the Candidate Firewall Product must continue to keep track of the date and time such that the date and time are accurate when electrical power is reapplied.

NOTE1 TO PE5 – This requirement is not intended to cover situations where electrical power is lost or removed while exercising any of the Administrative Functions^x.

NOTE2 TO PE5 – This requirement is not intended to cover situations where the Candidate Firewall Product hardware becomes faulty as a result of a loss or removal of power.

NOTE3 TO PE5 – In the event that the Candidate Firewall Product cannot meet this requirement without making remote time and date acquisition access requests, the Candidate Firewall Product must completely satisfy all requirements in TDC (Time and Date Acquisition).

LOGGING

LO7 – Log Access Control Rule Change Events – In the event that an Access Control Rule^{xi} is created or altered, the Candidate Firewall Product must have the capability to minimally log a statement indicating that the Access Control Rules^{xii} have been altered accompanied by the date and time^{xiii} the event occurred.

NOTE1 TO LO7 – Candidate Firewall Products do not have to go into any kind of detail about what additions or changes were made to the Access Control Rules^{xiv}.

FUNCTIONAL TESTING

FT3 – Testing All Configuration Modes – In the event that the security policy can be implemented on the Candidate Firewall Product using multiple configuration modes, each documented mode that is tested, once properly configured for the security policy, must demonstrate through testing that it properly enforces that security policy.

TIME AND DATE ACQUISITION

NOTE: This is a **CONDITIONAL** requirement based on whether the Candidate Firewall Product must acquire the Date and Time from an external source. If this is the case, then the requirements outlined in this section must be met.

TDC1 – NTP Time and Date Acquisition -- The Candidate Firewall Product must be capable of properly running NTP in symmetric active mode as defined in RFC 1305.

NOTE1 to TDC1 – The Baseline module Security Testing requirements will be applied to the Candidate Firewall Product's NTP implementation.

NOTE 2 to TDC1 – If the Candidate Firewall Product runs NTP in symmetric active mode but also uses client/server mode at startup, an administrative function to disable client/server mode at startup must exist

ICSA Labs

The Modular Firewall Certification Criteria



Required Services Security Policy - Corporate Category module - version 4.1

TDC2 – NTP Peering -- The Candidate Firewall Product must be capable of supporting multiple NTP peering topologies. At a minimum, the CFP should be capable of being configured to properly form NTP associations with two peers on the public network and two peers on the private network (four in total.)

NOTE1 to TDC2 -- The CFP must also be capable of being configured to form NTP associations with only two peers on the same network (public or private.)

NOTE2 to TDC2 -- The CFP must also be capable of being configured to form an NTP association with a single peer on either the public or private network.

TDC3 – Fixed Time and Date at Startup -- At every startup, before the time and date have been synchronized with an NTP peer, the Candidate Firewall Product must begin at the same fixed time and date

TDC4 – Upon synchronization with an NTP peer, the newly acquired time and date must be used by the Candidate Firewall Product as the timestamp for logged events as required by the Baseline module LO1 requirement.

TDC5 – Configuring NTP -- Administrative Functions must exist on the Candidate Firewall Product to:

- A. Disable NTP;
- B. Configure IP Addresses of NTP peers needed to meet each of the three topologies required by TDC2;
- C. Disable client/server mode NTP at startup if applicable.

TDC6 – Log Inability to Synchronize Time and Date -- The Candidate Firewall Product must have the capability to log all failed attempts to reach an NTP peer and to include the following data in a log for such an event:

- A. The current timestamp on the Candidate Firewall Product in accordance with the Baseline module LO2A requirement;
- B. A statement that a peer could not be reached;
- C. The IP Address of the NTP peer that could not be reached.

NOTE1 to TDC6 – The “current timestamp” may include no date. Further, it may reflect time relative to the fixed startup time in the event that time and date could not be set at startup.

TDC7 – Log NTP Time and Date Clock Resets -- The Candidate Firewall Product must have the capability to log each occasion where an NTP “step phase adjustment” causes the time and date clock on the Candidate Firewall Product to be reset and to include the following data in a log for such an event:

- A. The current timestamp on the Candidate Firewall Product before its clock is reset;
- B. The timestamp that the Candidate Firewall Product set its clock to;
- C. A statement that the clock was reset;
- D. The IP Address of the NTP peer(s) that the Candidate Firewall Product selected as its synchronization source.

NOTE1 to TDC7 – A “step phase adjustment” is defined in the NTP RFC 1305 and typically occurs only once at startup or during periods of network instability.

NOTE2 to TDC7 – If the Candidate Firewall Product implements the NTP clock-combining algorithm (RFC 1305 Appendix F), the IP Addresses of all peers used in computing the clock are required by TDC7,D.

TDC8 – Document Fixed Time and Date at Startup – The Candidate Firewall Product must indicate in written and/or electronic documentation the fixed time and date used by the Candidate Firewall Product prior to synchronizing with an NTP peer.

ⁱ Refer to DO1 in the Baseline module.
ⁱⁱ Refer to AD8 in this module.

- iii Refer to AD6 in this module.
- iv Refer to AD8 in this module.
- v Refer to AD6 in this module, AD1 in the Baseline module and, if applicable, to PE1,B in the Baseline module, and AD8 in the Management module.
- vi Refer to RSC2 in this module.
- vii Refer earlier in the module to this requirement.
- viii Refer to AD2 in the Baseline module.
- ix Refer earlier in the module to this requirement.
- x Refer to AD6 in this module, AD1 in the Baseline module and, if applicable, to PE1,B in the Baseline module, and AD8 in the Management module.
- xi Refer to AD6,A & C in this module.
- xii Refer to AD6,A & C in this module.
- xiii Refer to LO2,A and LO3 in the Baseline module for the date and time elements that must be recorded and for the precision with which they must be recorded.
- xiv Refer to AD6,A & C in this module.