ICSA Labs
Firewall Certification Criteria
Enterprise Module - Version 4.2

Document Version 1.1
October 28, 2015

www.icsalabs.com

Table of Contents

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 a 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.

Unless otherwise explicitly stated all testing will be conducted using an IPv4 network infrastructure. Any criteria requirements expecting IPv6 will be clearly outlined.

Finally, unlike the Residential, Small-Medium Business (SMB) or Corporate categories, NTP or SNTP is a **MUST** requirement in order to achieve Enterprise certification.

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

RSE2 – Enforcing the Required Services Security Policy

After configuring Access Control Rules, 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 request*s 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 – IPV4 and IPV6)
2. HTTP (IPV4 and IPV6)
3. HTTPS (IPV4 and IPV6)
4. SMTP (IPV4 and IPV6))
5. DNS and EDNS0 (may be hosted by the firewall – IPV4 and IPV6)
6. POP3 (IPv4 only)
7. IMAP(IPv4 only)
8. SSH (IPv4 only)

B. *Traffic* Permitted Outbound – The *Candidate Firewall Product* must support *access request*s from private and *service network clients* to services on *public network servers*. Such requests must be permitted for the following services:

1. TELNET (IPv4 only)
2. FTP (Active and Passive Mode – IPV4 and IPV6)
3. HTTP (IPV4 and IPV6)
4. HTTPS (IPV4 and IPV6)
5. SMTP (IPV4 and IPV6)
6. DNS and EDNS0
7. POP3 (IPv4 only)
8. IMAP(IPv4 only)
9. SSH (IPV4 and IPV6)

C. *Traffic* Permitted for *Candidate Firewall Product* -- The *Candidate Firewall Product* may permit *access request*s for the following services:

1. *Remote Administration access request*s from private, service and *public network clients* to the *Candidate Firewall Product*
2. Time and date acquisition *access request*s 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 *drop*ped or denied.

NOTE1 TO RSE2 – It is acceptable for *Candidate Firewall Product*s to require that one or more of the *servers* hosting required services in RSE2, A be located on the *service network*.

NOTE2 TO RSE2, B & C – The *Candidate Firewall Product* may require that private and *service network clients* use SOCKS4 or SOCKS5 to satisfy RSE2, 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 RSE2, A1 and B1 – Active EPRT and Passive EPSV modes for IPv6 required.

NOTE4 TO RSE2, D – RSE2, D does not apply to any services required elsewhere within this Enterprise criteria module.

RSE3 – 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* 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;
2. Enforce a security policy different than 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 *drop*ping or *deny*ing all other *traffic*.

B. Review the Access Control Rules.

C. Alter the Access Control Rules.

NOTE1 TO AD6, A2 - In addition to being configured for IPv6 services, the *Candidate Firewall Product* must have the ability to configure additional policy rules with the ability to block or allow packets by analyzing their source port, destination port, source address or destination address.

AD8 – Remote Administration

The *Candidate Firewall Product* must permit *Remote Administration* having the following characteristic in addition to that of AD5:

A. The *Remote Administration traffic* must be encrypted.

AD9 – Local Administration

The *Candidate Firewall Product* must permit Local Administration through an *Administrative Interface* in accordance with AD5.

AD10 – Administrative Accounts

The *Candidate Firewall Product* must be able to have multiple administrative accounts with varying levels of access.

NOTE TO AD10 – at a minimum one of these accounts must be able to be configured to have READ ONLY access.

Logging

LO7 – Log Access Control Rule Change Events

In the event that an Access Control Rule is created or altered, the *Candidate Firewall Product* must have the capability to minimally *log* a statement indicating that the Access Control Rules have been altered accompanied by the date and time the event occurred.

NOTE1 TO LO7 – *Candidate Firewall Product*s do not have to go into any kind of detail about what additions or changes were made to the Access Control Rules.

NOTE2 TO LO7 – Refer to LO2,A and LO3 in the Baseline module.

LO8 – Other Requirements

The *Candidate Firewall Product* must be able to be configured to meet all of the *logging* requirements as outlined in the HA, IPv6 and VoIP sections of this module, in addition to this section.

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 *mode*s, each documented *mode* that is tested, once properly configured for the *security policy*, must demonstrate through testing that it properly enforces that security policy.

NOTE1 TO FT3 - If HA or VoIP do not work in a given *mode*, this must be documented.

Time and Date Acquisition

The *Candidate Firewall Product* SHOULD implement NTP Time and Date Acquisition as enumerated below in requirements TDE1 – TDE8. In the event this is not possible then the CFP MUST meet the requirements enumerated in TDE9 – TDE17.

TDE1 – 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 TDE1 – The Baseline module Security Testing requirements will be applied to the *Candidate Firewall Product*'s NTP implementation.

NOTE 2 TO TDE1 – 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.

TDE2 – 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 TDE2 -- 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 TDE2 -- 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*.

NOTE3 TO TDE2 – The CFP must be capable of being configured to peer with each other as well as two other lower-stratum peers (*servers*).

TDE3 (Conditional) – 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.

NOTE TO TDE3 – the requirement is required if there IS NOT a battery backed up clock on the CFP.

TDE4 – Usage of Acquired Time

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.

TDE5 – 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 TDE2;
C. Disable client/server *mode* NTP at startup if applicable.

TDE6 – 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 TDE6 – 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.

TDE7 – 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 TDE7 – 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 TDE7 – 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 TDE7,D.

TDE8 (Conditional) – Document Time and Date at Startup

The *Candidate Firewall Product* must indicate in written and/or electronic documentation the time and date used by the *Candidate Firewall Product* prior to synchronizing with an NTP peer.

NOTE TO TDE8 – the requirement is required if there IS NOT a battery backed up clock on the CFP.
NOTE: In the event the *Candidate Firewall Product* cannot meet the TDE1 – TDE8 requirements, then the requirements as outlined in TDE9 – TDE17 MUST be met.

TDE9 – SNTP Time and Date Acquisition

The *Candidate Firewall Product* must be capable of properly running unicast client mode SNTP as defined in RFC 2030.

NOTE1 TO TDE9 – The Baseline module Security Testing requirements will be applied to the *Candidate Firewall Product*'s SNTP.

TDE10 (Conditional) – Document Time and Date at Startup

The *Candidate Firewall Product* must indicate in written and/or electronic documentation the time and date used by the *Candidate Firewall Product* prior to synchronizing with an SNTP or NTP server.

NOTE TO TDE10 – the requirement is required if there IS NOT a battery backed up clock on the CFP.

TDE11 – SNTP Servers

The *Candidate Firewall Product* must be capable of being configured to select an SNTP server to use from a configured list of at least two NTP *servers* on a dedicated network.

NOTE1 TO TDE11 -- The dedicated network must be a segment that has its own network interface on the CFP that is not used for any *traffic* other than CFP administrative, *logging* or other management *traffic*.

TDE12 (Conditional) – Fixed Time and Date at Startup

At every startup, before the time and date have been synchronized with an SNTP server, the *Candidate Firewall Product* must begin at the same fixed time and date.

NOTE TO TDE12 – the requirement is required if there IS NOT a battery backed up clock on the CFP.

TDE13 – Re-synchronization

The *Candidate Firewall Product* must be capable of being configured to periodically re-synchronize with the selected SNTP server often enough to prevent excessive drift.

NOTE1 TO TDE13 – In accordance with the Baseline module LO3 requirement excessive drift is considered to be one-half second or greater.

NOTE2 TO TDE13 – The *Candidate Firewall Product* must first attempt to re-synchronize to the SNTP server previously used for synchronization. Switching SNTP *servers* should only occur when the previously used SNTP server cannot be reached.

NOTE3 TO TDE13 – Regardless of the clock drift rate, the CFP must re-synchronize at least once per day. If the re-synchronization period is non-configurable, there must be written and/or electronic documentation specifying either a fixed period or the algorithm used to schedule re-synchronizations.

TDE14 – Usage of Acquired Time

Upon synchronization or re-synchronization with an SNTP server, 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.

TDE15 – Configuring SNTP

Administrative Functions must exist on the *Candidate Firewall Product* to:

A. Disable SNTP; and
B. Configure a list of SNTP server IP Addresses as required by TDE3.

TDE16 – Log Inability to Synchronize Time and Date

The *Candidate Firewall Product* must have the capability to *log* all failed attempts to reach an SNTP server 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 server could not be reached;
C. The IP Address of the SNTP server that could not be reached.

NOTE1 TO TDE16 – 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.

TDE17 – Log SNTP Time and Date Synchronizations

The *Candidate Firewall Product* must have the capability to *log* each occasion where the response from an SNTP server causes the time and date clock on the *Candidate Firewall Product* to be updated 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 in accordance with the Baseline module LO2A requirement;
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 SNTP server that the *Candidate Firewall Product* synchronized to.

Documentation

DO7 – Format of Log Messages

In addition to the Baseline DO5 requirement, documentation outlining the format of all *log* messages must be provided.

DO8 – Fixes and Upgrades

In the event the *Candidate Firewall Product* needs to be upgraded or have a fix applied to it, the effects of this upgrade and/or fix must be documented.

NOTE1 TO DO8 – said documentation must, at a minimum, include any changes to configuration and portability of configuration(s) across the upgrade/fix, whether a reboot or reset is required.

DO9 – HA Documentation

The following documentation must be provided:

A. CONDITIONAL -- If HA configuration is not part of the product's standard installation process, then additional documentation covering HA configuration is required.
B. CONDITIONAL -- If HA does not work in a given *mode* (e.g. NAT vs. routing vs. bridging), this must be documented.
C. Accurate Documentation – All *Candidate Firewall Product* documentation used for the purposes of testing may not be inaccurate.

DO10 – VoIP Documentation

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

A. Configuration Documentation -- The *Candidate Firewall Product* must include some measure of written and/or electronic guidance indicating how to properly configure the *Candidate Firewall Product* for VoIP functionality.
B. If VoIP does not work in a given *mode*, this must be documented.
C. Accurate Documentation – All *Candidate Firewall Product* documentation used for the purposes of testing may not be inaccurate.

High Availability Overview

This section captures, at a minimum, the High Availability (HA) capabilities expected of an Enterprise Firewall.

Vendor firewall products satisfying the requirements in this section will have to be able to correctly handle the transition from Active, Passive and Other states. Additionally the *Candidate Firewall Product* will be tested to ensure that its basic HA functionality does not introduce security vulnerabilities. Also, the product will be required to meet the Functionality, *Logging*, Reaction Time and Documentation requirements as outlined. Finally, the *Candidate Firewall Product* granted certification against the criteria contained within this document will be able to sustain a minimum of 66.6% of the number of simultaneous connections documented by the vendor.

High Availability State Definitions

The following definitions are used throughout the Requirements in relation to the state of a given unit. There is no requirement for the CFP to use this terminology.

Active – This unit is actively handling connections.

Passive – This unit is not actively handling connections but is ready to do so should the *Active* unit(s) become unable to continue handling connections.

Other – Also known as the "unknown" state. This is a catch-all to cover states where the unit is not Active or Passive. This may be due to a network or device failure which makes the unit unable to be Active or an administrative command to take the unit out of service.

High Availability Certification Requirements

HA01 -- HA Configuration

A) CFP must be capable of being configured in a 2 firewall unit (FW A and FW B) configuration in:

1. Active/Passive mode; or
2. OPTIONAL - Active/Active mode

B) Use of HA must not require using a *mode* (e.g. NAT vs. routing vs. bridging) which cannot meet all Baseline and Enterprise category criteria requirements.

NOTE1 TO HA01,A -- Use of Active/Active mode has the additional CONDITIONAL requirement HA06,C. In addition, some requirements are simplified by use of *Active*/*Passive* mode -- see HA NOTE to LO5.

HA02 -- HA Functional

1. Established TCP sessions must continue to work after a failure event has been artificially created. New connections for allowed RSSP services must work.

   Failure events:

   A) Power loss to Public Switch connected to FW A or FW B

   B) Power loss to Private Switch connected to FW A or FW B

   C) Power loss to FW A

   D) Power loss to FW B

2. CFP must be capable of sustaining a minimum of 66.6% of the documented number of simultaneous connections

NOTE1 TO HA02, 1 -- "Split-brain syndrome" (a loss of signal between FW A and FW B) will not be tested intentionally. However, if a product does not use a separate heartbeat/state link between FW A and FW B, then this scenario may be tested as a matter of course (e.g., if LAN-based heartbeat/state is the only available configuration, then split-brain will occur during failures of the private LAN).

NOTE1 TO HA02, 2 – The “documented number of simultaneous connections” will be determined based on information provided by the vendor. This information will become part of the final lab report posted to the ICSA Labs website.

HA03 -- HA Reaction Time

The following time limit must not be exceeded:

A) Failure event to failover of sessions: 65 seconds

NOTE1 TO HA03 – It is ICSA Labs’ intention to tighten this time limit in future revisions of these criteria.

NOTE2 TO HA03 – Should the CFP expire idle connections sooner than this time limit, the idle expiration time must not be exceeded.

HA04 -- HA Security

HA must not introduce vulnerabilities

A) Established sessions must be maintained.

B) After failover, half-open connections must either be discarded or be completed only if the handshake completes (i.e., half-open connections must not be "upgraded" to full open (established) automatically as a result of failover).

C) HA itself must not be vulnerable to induced or prevented failover. Spoofed HA messages must not be accepted.

NOTE1 to HA04,C -- A hypothetical attacker will have access to generate packets on either the private or *public network*s (but not a private FW A to FW B connection) and is assumed to have knowledge of the MAC and IP addresses in use. However, the attacker will not have the ability to "sniff" the network (e.g., will not have access to static authenticators or the ability to replay packets).

HA05 -- HA Event *Logging*

CFP must have the capability of *logging* when a Passive unit changes its HA state.

A) When a Passive unit enters an Other state.

B) When a Passive unit becomes Active.

HA06 -- HA Administration

CFP must have the following *administrative functions*:

A) Method to determine current status (e.g., Active or Passive) of each unit

B) Method to make a given unit Active on demand

C) CONDITIONAL -- In Active/Active mode, a Method to gracefully "fail" a unit to make it non-active (either Passive or the Other state)

NOTE1 TO HA06,B -- In Active/Passive mode, if the mechanism is such that one makes a unit *Active* by making the other unit Passive, that is acceptable.

NOTE1 TO HA06,C -- There is no requirement for a specific out-of-service state, but such a state is acceptable as "non-active". It is also acceptable for the "failed" unit to go into a *Passive* state.

High Availability Notes to Other Criteria

HA-related notes to Baseline and Enterprise module criteria elements:

Baseline elements:

HA NOTE TO LO1,G -- Required *Log* Events -- A startup *log* message is required. Both units must *log* a startup message. If a unit *log*s a state change message at startup, that single message may be used to meet both the LO1,G (startup) and HA05,B (state change to Active) *log* message requirements as long as it is possible to determine from the message that the state being reported is the result of a unit startup.

HA NOTE TO LO5 -- *Log*s Sent to Separate *Candidate Firewall Product* Component -- If *log*s are sent to a separate CFP component, a unique identifier is required. In *Active*/*Passive mode* it is acceptable to use an identifier shared by both the *Active* and *Passive* units for events which occur on the *Active* unit as a result of it being the *Active* unit. Administrative connections to a specific unit must use a unique identifier. In *Active*/*Active mode*, a shared identifier is never acceptable.

HA NOTE TO DO1 -- HA NOTE to DO5 -- *Log* Event Dispositions Defined -- Documentation defining *log* event dispositions is required. However, provided that the *log* messages are self-explanatory, this is not required for the events listed in HA05.

Enterprise category elements:

HA NOTE TO AD9 -- Local Administration -- The CFP must have a local *Administrative Interface*. Each HA unit must have its own local *Administrative Interface*.

Voice over IP (VoIP) Overview

This section captures, at a minimum, the Voice over IP (VoIP) capabilities expected of an Enterprise Firewall.

Vendor firewall products satisfying the requirements in this section will have to be able to correctly handle SIP, RTP and TFTP *traffic*. Additionally the *Candidate Firewall Product* will be tested to ensure that its basic VoIP functionality does not introduce security vulnerabilities and that the related network *traffic* is able to traverse the *Candidate Firewall Product* in various network topo*log*y scenarios. Also, the product will be required to meet the Administration, *Logging* and Documentation requirements as outlined. Finally, the *Candidate Firewall Product* granted certification against the criteria contained within this document will be able to protect itself against SIP based Denial of Service attacks.

Voice over IP (VoIP) Certification Requirements

VP01 – Required Services Security Policy

The *Candidate Firewall Product* must be capable of allowing the following:

A. SIP
B. RTP
C. TFTP

Note1 to VP01,B – RTP sessions must be dynamically allowed as appropriate based on inspection of SIP *traffic*.

VP02 – Functional Testing

While testing the *Candidate Firewall Product* it must demonstrate that it is capable of the following:

A. To the extent the *Candidate Firewall Product* is involved, it must be capable of properly supporting and not interfering with the following:
    1. Make and receive calls
    2. Transfer to Park/to Hold
    3. Call Forwarding
    4. Multiple lines
    5. Voicemail
    6. Peer registration
    7. Phone registration

B. QoS settings in IP header (e.g. DiffServ) must be maintained OR the *Candidate Firewall Product* must provide functionality to mark packets in order to effectively maintain QoS.
C. VoIP configurations must not require using a *mode* which cannot also meet all Baseline and previously tested RSSP criteria requirements.
D. The *Candidate Firewall Product* must be able to properly handle the following network topologies and situations:
    1. *Candidate Firewall Product* is between a SIP phone and a PBX
        i. public SIP phone and private PBX
        ii. private SIP phone and public PBX
    2. *Candidate Firewall Product* is between two PBXs
    3. Situations where use of NAT/PAT, on the *Candidate Firewall Product* itself or elsewhere in the network path, causes two SIP phones to externally appear to have the same IP address

VP03 – Security Testing

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

A. The protocol in use must not create other security issues during call setup, call teardown or while the call is in progress; and
B. It is not rendered inoperable by any SIP DOS attacks.

VP04 – Administration

The *Candidate Firewall Product* must have the following *Administrative functions*:

A. Determine/provide a listing of dynamically opened RTP sessions

VP05 – Logging

The *Candidate Firewall Product* must be capable of *logging*:

A. Allowed SIP, RTP, and TFTP *traffic* as per the Baseline criteria LO1,A and LO1,B.

NOTE1 TO VP05 – In accordance with the Baseline criteria L02, *log* messages must include Date and Time, Protocol, Source and Destination IP addresses and port numbers, and Disposition of the Event.

IPv6 Overview

This section captures, at a minimum, the IPv6 capabilities expected of an Enterprise Firewall.

Vendor firewall products satisfying the requirements in this section will have to meet requirements as outlined in the Module Overview found at the beginning of this document. The difference is that these requirements will be tested using IPv6 as the mode of transport.

IPv6 Configuration

The *Candidate Firewall Product* will be configured in a dual stack (IPv4/IPv6) mode. Testing will be based on IPv6 *traffic* without authentication and encryption.

IPv6 Administration

V6AD2 – Blocking Remote Administration

The *Candidate Firewall Product* must be capable of being configured to block all Remote Administrative access via IPv6.

IPv6 Security

V6ST1 – Administrative Access

The *Candidate Firewall Product* must demonstrate through testing that no unauthorized control of its *Administrative Functions* can be obtained.

NOTE1 to V6ST1 – No *administrative interface* access via IPv6 is required. However, if an *administrative interface* used to meet Baseline and Enterprise module *remote administration* requirements via IPv4 is also available via IPv6, it will be tested via IPv6 as well.

NOTE2 TO V6ST1 -- The *Candidate Firewall Product* must maintain Remote Administrative access via IPv4. The rational for this requirement is that existing IPv4 infrastructure is better understood and monitored than new IPv6 infrastructure. Over time, ICSA Labs intends to review this requirement as IPv6 security issues become better known and mitigated. See http://www.securityfocus.com/news/11406 as an example of the issues surrounding IPv6 access.

V6ST6 – Fragmentation Handling

The *Candidate Firewall Product* must demonstrate through testing that it has the capability, though it need not be the default behavior, to:

A. For all services including the set of Required Services, prevent invalid or incomplete fragmented datagrams from traversing the *Candidate Firewall Product*. Three acceptable options are:
    1. Cache IPv6 datagram fragments, verify that a complete set of valid fragments for a datagram has arrived, verify that the hypothetically reassembled datagram is allowed by the configured Security Policy, then forward the original set of fragments (typical option for packet-oriented devices acting as an IPv6 router); or
    2. Correctly reassemble a complete set of valid fragmented IPv6 datagrams on the *Candidate Firewall Product*, forward the *traffic* only if allowed by the configured Security Policy, emitting fragments only if warranted by the next hop MTU (typical option for proxy-oriented devices acting as an IPv6 host); or
    3. *Drop* all IPv6 datagram fragments arriving at a *Candidate Firewall Product* interface (not recommended, this option may be removed in future revisions of this criteria).
B. Forward ICMPv6 Packet Too Big messages received by the *Candidate Firewall Product* when the returned IPv6 header corresponds to a known session;
C. Not forward ICMPv6 Packet Too Big messages received by the *Candidate Firewall Product* when the returned IPv6 header does not correspond to a known session; and
D. Generate ICMPv6 Packet Too Big messages when appropriate.

NOTE TO V6ST6,B and V6ST6,C -- For the purpose of determining if an ICMPv6 Packet Too Big message should be forwarded, for an IPv6 header to correspond to a known session, only the combination of Source and Destination addresses are required to match. It is, however, recommended that if a protocol header is contained in the returned IPv6 header, that the information in that header is also used to make this determination.

NOTE TO V6ST6, A, 3, V6ST6,B and V6ST6,C – These recommendations will be a requirement on October 27, 2011.

V6ST7 – Blocking of Packets

The *Candidate Firewall Product* must have the ability to block packets with a Routing Header type 0. It is unacceptable for the *Candidate Firewall Product* to block ALL Routing Headers in order to satisfy this requirement. Additionally, the *Candidate Firewall Product* must have the capability to selectively block any packet by extension header or upper layer next header.

IPv6 Logging

V6LO2 – 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 *Candidate Firewall Product* 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 *Candidate Firewall Product* for each event in the *log* must consist of the hour, the minute and the second.
B. Indication *traffic* is IPv6;
C. Source IPv6 Address - from the *Candidate Firewall Product*'s perspective;
D. Destination IPv6 Address - from the *Candidate Firewall Product*'s perspective;
E. Next Header;
F. Extension headers;
G. Source Port (TCP and UDP);
H. Destination Port (TCP and UDP);
I. Message Type (ICMPv6);
J. Disposition of the Event.

NOTE1 TO V6LO2,A – Any date formatting that is outlined in ISO 8601:2004 (Representation of Dates and Times) will be acceptable provided required data is present.