1 Module Overview

This module is targeted at firewall products designed to protect:

- a small company;
- a branch or remote office within a company; and
- a telecommuter.

The common element shared by these is that they require Remote Administration over an encrypted link from a public source. Additionally, 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 while allowing a set of common services outbound. 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. Any use of administrative functions on the product is preceded by successful authentication. The date and time will persist in the event that there is a loss or removal of power.

2 Module Requirements

REQUIRED SERVICES SECURITY POLICY - SMB CATEGORY

RSB1 – Enforcing the Default Security Policy – After being installed according to the Installation Documentation, 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 Administration 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 RSB1 – A complete deny-all inbound policy is an acceptable way to meet RSB1,A.

NOTE1 TO RSB1 – The Candidate Firewall Product may require that private and service network clients use SOCKS4 or SOCKS5 to satisfy RSB1,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.

B. Minimally Permit Common Services Outbound – The Candidate Firewall Product must permit access requests from private and service network clients to public network servers for at least the following services:

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

NOTE1 TO RSB1 – The Candidate Firewall Product may require that private and service network clients use SOCKS4 or SOCKS5 to satisfy RSB1,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.

RSB2 – Enforcing the Required Services Security Policy – After configuring the 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 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

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:

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

C. All other non-Remote Administration iv traffic from both private, service and public network clients directed to or through the Candidate Firewall Product must be dropped or denied.

NOTE1 TO RSB2 – It is acceptable for Candidate Firewall Products to require that one or more of the servers hosting required services in RSB2,A be located on the service network.

NOTE2 TO RSB2 – The Candidate Firewall Product may require that private and service network clients use SOCKS4 or SOCKS5 to satisfy RSB2,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 RSB2,C – RSB2,C 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.

RSB3 – 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 implement the Required Services Security Policy.
B. Review the Access Control Rules.
C. Alter the Access Control Rules.

AD7 – Remote Administration – The Candidate Firewall Product must permit Remote Administration having the following characteristics in addition to that of AD5:

A. Remote Administration must be configurable from a public client; and
B. The Remote Administration traffic must be encrypted;
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\(^{\text{viii}}\).

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.

---

\(^{\text{i}}\) Refer to DO1 in the Baseline module.
\(^{\text{ii}}\) Refer to AD7 in this module.
\(^{\text{iii}}\) Refer to AD6 in this module.
\(^{\text{iv}}\) Refer to AD7 in this module.
\(^{\text{v}}\) 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.
\(^{\text{vi}}\) Refer to RSB2 in this module
\(^{\text{vii}}\) Refer earlier in the module to this requirement.
\(^{\text{viii}}\) 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.