1 Module Overview

This module is targeted at vendor firewall products designed to provide access to the Internet for the home or consumer market. Firewall products satisfying the requirements in this module will not necessarily include functionality to configure Access Control Rules. Instead, a default security policy permitting at least a handful of standard services outbound from private hosts must be in effect such that upon installation, the product is ready to use. The product may retrieve its public IP address from a remote source. Also, once the product is properly installed a security policy denying all traffic inbound originating from the public must be in effect. The product would have to offer the capability to be administered from some non-local source on the private LAN. Finally, though the capability exists for administrators to authenticate at the product, there is no requirement stipulating that authentication must occur before access to the administrative functions is permitted.

2 Module Requirements

REQUIRED SERVICES SECURITY POLICY - RESIDENTIAL CATEGORY

RSA1 – Enforcing the Required Services Security Policy – After being installed according to the Installation Documentation, the Candidate Firewall Product must immediately enforce the Required Services Security Policy as defined below:

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

B. Minimally Permit Common Services Outbound – The Candidate Firewall Product must permit access requests from private 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

C. Remote Public IP Address Discovery – It shall be permissible for the Candidate Firewall Product to send and receive traffic on the public network related to acquiring the public IP address of the Candidate Firewall Product.

D. Time and Date Determination – It shall be permissible for the Candidate Firewall Product to send and receive traffic related to acquiring the current time and date.

NOTE1 TO RSA1 – The Candidate Firewall Product may require that private network clients use SOCKS4 or SOCKS5 to satisfy RSA1,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.

NOTE2 to RSA1 – There are numerous permissible means in RSA1,C to obtain or retrieve a public IP address for the Candidate Firewall Product.
RSA2 – 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

AD4 – Remote Administration – The Candidate Firewall Product must permit Remote Administration from a private client in accordance with AD3".

---

i Refer to DO1 in the Baseline module.

ii Refer to this requirement in the Baseline module.