digital™

Software Product Description

PRODUCT NAME: AltaVista Firewall Version 2.1 for BSD/OS SPD 56.36.01

DESCRIPTION

AltaVista™ Firewall for BSD/OS® provides a secure and flexible connection between a trusted private IP network and an insecure public network, such as the Internet. It may also be used to secure the connection between portions of the private network within an organization.

AltaVista Firewall for BSD/OS consists of a suite of application gateways for controlling access between networks. It provides utilities for managing data logging, reporting, and user authentication, as well as a firewall status monitoring system with built-in alarms. It also provides a comprehensive graphical user interface (GUI) to ease firewall configuration and management.

AltaVista Firewall for BSD/OS provides trusted application gateways to allow users access to most common services on the Internet, including file transfer (FTP), remote terminal sessions (TELNET, TN3270), electronic mail (SMTP), the World Wide Web (HTTP), News (NNTP), and Finger. It also includes a user-configurable generic TCP gateway. The application gateways enforce robust security checks to protect against unauthorized access. The FTP and TELNET gateways support operation in both transparent and non-transparent modes.

AltaVista Firewall for BSD/OS provides a selection of predefined security policies appropriate to each application gateway, which can be set up *via* the GUI. In addition, customized security policies can be developed *via* the GUI for the FTP, TELNET, and Finger application gateways. Security policies can be configured to restrict access to specified groups of users and servers, as well as on the basis of time.

User-based authentication is available for FTP and TELNET access to and from the internal network. This allows access to be restricted to individual users. A variety of authentication methods is provided, including handheld authentication cards, once-off passwords, and reusable passwords. Handheld authentication cards are not included with the AltaVista Firewall for BSD/OS product, and must be purchased separately.

October 1996
AE-QZSTB-TE

The firewall performs comprehensive logging of all events relating to the operation of the firewall. A wide range of summary and detailed reports can be generated from the information in the log files.

AltaVista Firewall for BSD/OS supports automatic, real-time alarms to alert the system manager of unusual or potentially threatening events on the firewall. The alarm system monitors the system log files for suspicious events, and triggers one or more alarm actions in response.

AltaVista Firewall for BSD/OS provides a comprehensive graphical user interface, including support for all stages of firewall configuration and management. The user interface includes a comprehensive online help system, including context-sensitive help on all screens.

AltaVista Firewall for BSD/OS supports the use of firewalls within a firewall, where an organization requires that a portion of its private network must be secured using an internal firewall. This allows the secure portion of the private network to have secure connectivity to the remaining portion of the private network, and also connectivity to the external network *via* a second firewall.

AltaVista Firewall for BSD/OS is based on technology that has been tried and tested in Digital's own network for over five years.

AltaVista Firewall for BSD/OS runs on a dedicated hardware system. To maximize the security of the firewall, Digital recommends that there are no user accounts on the system on which Digital Firewall for BSD/OS is installed, and that no other applications run on the system. The system should also be secure from physical intrusion.

The following sections describe the features of the AltaVista Firewall for BSD/OS Version 2.1 in more detail.

Application Gateways

The firewall uses application gateways to provide users on the internal network with secure connectivity to the public network. Robust security checking protects the internal network against unauthorized access from the public network, and can also be configured to prevent access to the public network from the internal network, if required.

The firewall also controls the times at which each application gateway is available. You can configure each gateway to be available all the time; or only during specified business hours; or only outside specified business hours; or at specific times on named days.

Application gateways are provided for the following services:

- FTP

  The FTP application gateway can be used in both non-transparent mode and transparent mode (for outbound connections only). It provides support for both command line and windows-based FTP clients. The FTP gateway can be configured to control the FTP operations that can be performed, and hence the direction of data transfer. For example, the application gateway can control the ability of users to pull (GET) files or to push (PUT) files. Access can also be limited to users who are authenticated.

- Remote Terminal Service (TELNET)

The TELNET application gateway can be used in both non-transparent mode and transparent mode (for outbound connections only). The gateway includes support for TN3270 emulation. Access can also be limited to users who are authenticated.

- Electronic Mail

  The electronic mail gateway acts as a mail relay for SMTP mail between the external and internal networks. Incoming mail for the domain protected by the firewall is forwarded to a mail hub within the internal network for delivery. The mail gateway inspects the SMTP commands and message envelope to prevent attempts to subvert the firewall or the internal network.

- World Wide Web

  The World Wide Web application gateway acts as a proxy for users in the internal network. Internal users configure their World Wide Web browsers to use this gateway to access Web sites located on the external network. The World Wide Web gateway includes support for SSL and can be configured to support data caching to improve response for heavily-accessed Web sites. The gateway includes support for HTTP, gopher, WAIS, FTP, HTTPS, and SNEWS URLs. The World Wide Web application gateway uses the FTP application gateway to process FTP URLs, so that the security policy for FTP cannot be circumvented.

- News (nntp)

  The News application gateway acts as a relay between an internal News server and a News server located on the external network. The gateway can be configured to support outbound-only connections, inbound-only connections, or two-way connections.

- Finger

  The finger application gateway prevents users on the public network from accessing the internal network using the finger command.

- Generic TCP application gateway.

  The firewall also provides a customizable generic application gateway, which provides secure TCP connections to services which do not use a dedicated application gateway. The generic gateway enables the firewall administrator to set up secure connections between two named hosts, with each connection limited to a single service.

Security Policies

The FTP, TELNET, and Finger application gateways support custom security policies defined by the firewall administrator. A custom policy is defined by a set of rules. Each rule contains the following elements:

- A group of named users to whom the rule applies. You can also specify the hosts from which the users connect.

- A group of named servers to which the users connect. You can also specify a port number for a service on the server.

- Whether the rule allows the users to use the service or denies them from using it.
- For the FTP gateway only, the sets of FTP commands to which the rule applies.

Groups of named users and groups of named servers can be created through the user interface.

Sets of predefined security policies are provided for the FTP, TELNET, World Wide Web, and Finger gateways, as follows:

- FTP

  The following predefined security policies are available to control access from the internal network:

  – No access.

  – Allow authenticated ‘‘GETs’’ only.

  – Allow authenticated ‘‘GETs’’ and authenticated ‘‘PUTs’’.

  – Allow ‘‘GETs’’ and authenticated ‘‘PUTs’’.

  – Allow ‘‘GETs’’.

  – Allow ‘‘GETs’’ and ‘‘PUTs’’.

  The following predefined security policies are available to control access from the public network to the internal network:

  – No access.

  – Allow authenticated ‘‘GETs’’ and ‘‘PUTs’’.

  The FTP application gateway also supports custom security policies, as described in the next section.

- TELNET

  The TELNET application gateway provides a single set of predefined security policies that control access both from the internal network and from the external network. The following security policies are available:

  – No access from inside or outside.

  – Allow authenticated access from inside out. Deny all access from outside.

  – Allow authenticated access from inside out. Allow authenticated access from outside.

  – Allow access from inside out. Deny all access from outside.

  – Allow access from inside out. Allow only authenticated access from the outside.

  The TELNET application gateway also supports custom security policies, as described in the next section.

- World Wide Web

The World Wide Web application gateway prevents users on the public network from accessing the internal network, but allows secure access from the internal network to Web services on the public network. The following predefined security policies are provided:

  – No access.

  – Only users inside the firewall may use the World Wide Web gateway.

- Finger

  The following security policies are available to control access from the internal network to the public network:

  – No access.

  – Only users inside the firewall may use finger.

  The Finger application gateway also supports custom security policies, as described in the next section.

User-based Authentication

The firewall supports user-based authentication, using a variety of authentication methods. The following methods of user-based authentication are supported:

- Digital Pathways SecureNet Key (SNK)
- Security Dynamics SecurID cards
- Racal Watchword keys
- Bellcore S/Key
- ‘‘Once-off’’ passwords
- Reusable passwords (supported for outbound connections only)

The GUI provides an authentication user management system, with a step-by-step guide to configuring the authentication methods (that is, programming a handheld authentication card or setting a password).

To use any of the authentication methods that require handheld cards, you must purchase the handheld cards separately. To use Security Dynamics SecurID cards, you must also purchase the ACE/Server server software separately. The server software for the other authentication methods is included in the AltaVista Firewall for BSD/OS product.

Logging

All firewall components perform data logging when in operation. This ensures that comprehensive records of firewall usage are maintained in log files. The firewall log system automatically manages data logging and log file archiving. The firewall logging system monitors log file disk space and issues an alert if a predefined limit is exceeded. These features are user-configurable.

Reporting

The firewall generates reports, which give a summary of the usage of the firewall and of individual services. Reports can be viewed on the GUI, or mailed automatically at regular intervals to a specified list of users.

Security Alarms

An alarm system continually monitors the firewall in real time, and generates automatic alarms to alert the system administrator to unusual or potentially threatening events. Each alarm triggers one or more alarm actions, which include mailing or paging the system administrator, raising the security status of the firewall, blacklisting the remote host from which the event was generated, and shutting down individual services or the whole firewall. AltaVista Firewall for BSD/OS is installed with a default set of alarms, which are user-configurable.

The firewall uses a color-coded security status to indicate whether the firewall is under attack. There are four security statuses: green, yellow, orange, and red. The security status can be raised automatically by alarms, or manually by the system administrator.

Graphical User Interface

A comprehensive graphical user interface (GUI) allows the system administrator to perform all initial configuration, administration, and management tasks. The GUI is displayed in a window of the Netscape Navigator Web browser, and consists of multiple frames. Separate frames show the current status of the firewall, and the most recent events that triggered alarms.

The Netscape browser is protected by password. The GUI is also protected by a login and a timeout feature. After a specified period, the GUI times out and requires the user to log in again. This reduces the risk of intrusion if the GUI is left unattended. The timeout period can be configured or the timeout can be switched off, as required.

The product includes extensive online help, including task-oriented help, context-sensitive help on all significant screens in the user interface, and reference help.

“IP Spoofing” Software

The firewall product incorporates dedicated software to prevent so-called ‘‘IP spoofing’’ attacks. All packets that are received on the external network interface of the firewall but appear to originate from an address on the internal network are rejected.

Dependencies

AltaVista Firewall for BSD/OS requires that you configure other computer systems to perform specific roles, as follows:

- A system in the internal network must be configured as an internal mail hub. This system must be capable of delivering mail to all systems within the internal network.
- Depending on the configuration of the domain name service, it may be necessary to configure a system in the internal network as a primary name server.

HARDWARE REQUIREMENTS

Processors Supported:

AltaVista Firewall for BSD/OS runs on a 486- or Pentium-based personal computer (PC). The system must include one SCSI or IDE hard disk, one 3.5 inch diskette drive, and one SCSI or IDE CD-ROM drive. The system must also use supported network cards, graphics board, and SCSI driver, as listed below.

Supported Network Cards

The system on which you install the AltaVista Firewall for BSD/OS must have two network connections. It is recommended that one of these is an Ethernet or FDDI connection. The other connection can be a second Ethernet connection, or a Serial Line Internet Protocol (SLIP) or Point-to-Point Protocol link.

The following network cards are supported:

- NE-1000[1] and NE-2000[2] Ethernet cards, and compatible clones
- 3Com 3c501, 3c503, 3c505, 3c507, 3c509[3], 3c579, 3c590, and 3c595 Ethernet cards
- 3Com TokenLink III
- Allied Telesis RE2000/AT-1700 series
- Digital DE434, DE435, DE450, and DE500 PCI Ethernet cards
- Digital DE425 EISA Ethernet card
- Digital DEFEA-xx EISA FDDI cards
- Digital DEFPA-xx PCI FDDI cards
- HP EtherTwist PC Lan Adapter/16 Plus
- IBM TRA 16/4 token ring adapter
- Intel EtherExpress 16
- SMC EtherPower 10 and 100 Mb/s
- TNIC-1500 Ether from South Coast Computing Services
- Western Digital/SMC family cards

---

[1] Although hardware support for this network card is included in the AltaVista Firewall product software, it is not recommended that you use this software. The software is not fully supported, and may cause serious system problems, including loss of files.

[2] Some NE-2000 cards that use software configuration utilities rather than jumpers fail to work when a midi port is also configured.

[3] On systems that support Plug and Play, the Plug and Play feature must be disabled on the 3C509B card.

Supported Graphics Boards

Graphics boards that use the following graphics chips are supported:

- Alliance AS 3210 and AS6410
- ARK 1000VL, 1000PV, and 2000PV
- ATI ATIVGA, ATI38800, ATI68800, and ATI88000
- Advanced Logic 2101, 2228, and 2301
- Chips & Technology 82C453, 82C480, 82C481, F64300, F64310, F65530, F65535, F65540, and F65545
- Cirrus GD5420, GD5422, GD5424, GD5426, GD5428, GD5429, GD5430, and GD5434
- Compaq TRITON, ORIOL, and ARIEL
- IBM 8514/A, XGA, and XGA-2
- IIT AGX014 and AXG015
- Matrox TITAN, ATHENA, STORM, and ATLAS
- No. 9 I-128
- Oak OTI077, OTI087, and OTI107
- S3 86C732, 86C764, 86C801, 86C805, 86C864, 86C866, 86C868, 86C911, 86C928, 86C964, 86C968, 86C805i, and 86C924
- Trident TGUI9400, TGUI9420, TGUI9440, TVGA8900B, TVGA8900C, TVGA8900CL, TVGA8900D, and TVGA9200
- Tseng ET4000, ET4000/W32, ET4000/W32i, and ET4000/W32p
- Weitek P9000, P9100, W5186, and W5286
- Western Digital WD90C30, WD90C31, WD90C33, WD9500

Supported SCSI Drivers

The following SCSI drivers are supported:

- Buslogic 32-bit SCSI controller
- Adaptec 152x SCSI controller
- Adaptec 154x SCSI controller

Disk Space Requirements:

At least 500M bytes of disk space is required on the hard disk for installation and use of the AltaVista Firewall for BSD/OS. 1 gigabyte of disk space is recommended. These sizes are approximate; actual sizes may vary depending on the user's system environment, configuration, and software options.

AltaVista Firewall for BSD/OS creates extensive log files as part of its normal operation. More space may be required, depending on the configuration of the individual site and the level of usage of AltaVista Firewall for BSD/OS.

Memory Requirements:

AltaVista Firewall for BSD/OS requires a minimum of 16M bytes of memory.

SOFTWARE REQUIREMENTS

The BSD/OS operating system is supplied and installed as part of the AltaVista Firewall for BSD/OS product. The installation procedure deletes all existing software on the hard disk of the PC before installing the BSD/OS operating system and AltaVista Firewall for BSD/OS software. For this reason, there are no software requirements.

GROWTH CONSIDERATIONS

The minimum hardware/software requirements for any future version of this product may be different from the requirements for the current version.

DISTRIBUTION MEDIA

This product is available on CD-ROM. The product kit includes a CD-ROM and a floppy diskette from which the PC can be booted under BSD/OS. The printed documentation for this product can be ordered separately.

ORDERING INFORMATION

Software Media, License and Documentation:
50 Nodes: QB-5C6AA-SB
200 Nodes: QB-5C6AA-SC
Unlimited Nodes: QB-5C6AA-SD

Software Licenses:
50 Nodes: QM-5C6AA-AB
200 Nodes: QM-5C6AA-AC
Unlimited Nodes: QM-5C6AA-AD

The above information is valid at the time of release. Please contact your local Digital office for the most up-to-date information.

SOFTWARE LICENSING

This software is furnished under the licensing provisions of Digital Equipment Corporation's Standard Terms and Conditions. For more information about Digital's licensing terms and policies, contact your local Digital office.

Possession, use, or copying of the software described in this publication is authorized only pursuant to a valid written license from Digital or an authorized sublicensor.

SOFTWARE PRODUCT SERVICES

In addition to standard Software Product Services (SPS) remedial services, consulting services for planning, designing, and implementing a custom security system are also available. For more information, contact your local Digital office.

SOFTWARE WARRANTY

Warranty for this software product is provided by Digital with the purchase of this software package.

This product is intended to assist customers in maintaining an appropriately secure systems environment when used in conjunction with customers' vigilant operational security practices. Digital does not guarantee or warrant that the use of this product will provide complete security protection for customers' systems.