digital

AltaVista Firewall
Windows NT AlphaServer 800

DIGITAL HiTest Notes

Part Number: EK-HAFNF-HN. A01

April 1998

Revision/Update Information: This is a new document.

Digital Equipment Corporation
Maynard, Massachusetts

April 1998

Table of Contents

Figures

Tables

Preface

This document provides an overview of DIGITAL HiTest Suites and detailed technical information about the AltaVista Firewall Windows NT AlphaServer 800 HiTest Suite. This information includes the HiTest AppSet, the HiTest Foundation, configuration details, installation instructions, tuning parameters, problems encountered and their solutions, tests and test results, and system diagrams. Together, a HiTest Foundation and HiTest AppSet (Application Set) comprise all of the components in a HiTest Suite. The HiTest Foundation includes the hardware, operating system, middleware, and database software. The HiTest AppSet contains a collection of software specific to one class of customer solutions.

Audience

Primary users of this document are DIGITAL and Partners sales representatives and technical support personnel. Secondary audiences include product managers, customers, and the personnel responsible for installing, setting up, and operating a DIGITAL HiTest Suite.

Organization

This document is organized as follows:

Chapter Title	Description
Chapter 1 – Advantages of DIGITAL HiTest Suites	Provides a summary of the benefits of DIGITAL HiTest Suites and an overview of the Suite covered in this document.
Chapter 2 – About This DIGITAL HiTest Suite	Describes the specific characteristics of this HiTest Suite.
Chapter 3 – Configuration Data	Includes tables of configuration data about the hardware and software components that define the DIGITAL HiTest Template, and special configuration rules if any.
Chapter 4 – System Installation and Setup	Provides information for installing and setting up this DIGITAL HiTest Suite.
Chapter 5 – Tests and Results	Describes how the tests were set up including database organization, where data and programs were placed, and how the tests were run. It also describes system limits and characterization data.
Chapter 6 – Problems and Solutions	Discusses any problems and solutions that were discovered during testing.
Chapter 7 – Detailed Hardware Configuration	Contains more detailed information about the configuration of the hardware and software components listed in the Configuration Data chapter.

Customer Feedback

What our readers think of this or any other DIGITAL documentation is important to us. If you have any comments, we would appreciate hearing from you. Send your comments to: *reader-comments@digital.com*.

Please reference the complete document title and part number (EK-HAFNF-HN. A01) in your correspondence about this document.

Ordering Information

Copies of this and other DIGITAL documents can be ordered by calling 1-800-DIGITAL.

This document and other HiTest documents can be downloaded from the DIGITAL HiTest web site, which also provides access to other HiTest information such as configuration tools and parts updates.

`http://cosmo.tay.dec.com/public/configsys/config_systems.htm`

You can also visit the Technical Support Center web page, which provides additional information such as pointers to benchmark centers and major technical training and events:

`http://cosmo.tay.dec.com` (Intranet)
`http://www.partner.digital.com:9003/cgi-bin/comet` (Internet)

Related Documents

This document references the following manuals:

- *AlphaServer 800 Owner's Guide* (order number EK-ASV80-UG)

  This document is available in PostScript (.ps) and Adobe PDF (.pdf) formats. Both formats can be accessed from the DIGITAL AlphaServer 800 web site at:
  `http://www.digital.com/info/alphaserver/tech_docs/alphasrv800/`

  Choose AlphaServer Owner's Guide from the list of documentation.

- *AlphaServer 800 Technical Summary*

  This document is available in HTML, PostScript (.ps) and Adobe PDF (.pdf) formats. All formats can be accessed from the DIGITAL AlphaServer 800 web site at:
  `http://www.digital.com/info/alphaserver/tech_docs/alphasrv800/`

  Choose AlphaServer Technical Guide from the list of documentation.

- *AltaVista Firewall Windows NT Prioris MX DIGITAL HiTest Notes* (order number EK-HAFNM-HN)

  This document is also available in .DOC, .PDF and .HTML formats at:
  `http://cosmo.tay.dec.com`

The following documentation is provided with the respective software:

- *Microsoft Windows NT Server Start Here (Basics and Installation)*
- *AltaVista Firewall 97 Installation Guide*
- *AltaVista Firewall 97 Administrator's Guide*

1
Advantages of DIGITAL HiTest Suites

This chapter describes what a HiTest Suite is, the suite components and advantages, and customer add-ons.

What Is a DIGITAL HiTest Suite?

DIGITAL HiTest Suites are guidelines for configuring a set of prequalified computer systems. A HiTest Suite often contains all the hardware and software needed for a complete customer solution. DIGITAL HiTest Suites can be used as a basis for configuring systems that satisfy a wide set of customer requirements. Typically, Suites target specific markets such as data warehousing or security management.

In each HiTest Suite, the components are selected and the configurations designed to ensure system reliability, application performance, and ability to upgrade. The suite's hardware and software components have been successfully tested for interoperability.

The specifications for allowed ranges of hardware and software components, part numbers, description, and revision information are listed in the *DIGITAL HiTest Template* tables in Chapter 3.

DIGITAL HiTest Suite Components

The AltaVista Windows NT AlphaServer 800 HiTest Suite contains two groups of components: the *DIGITAL HiTest Foundation* and the *DIGITAL HiTest AppSet.*

The DIGITAL HiTest AppSet contains application software unique to the targeted market. The DIGITAL HiTest foundation contains the operating system software and hardware and can be used as a configuration guideline for the base platform for many applications and target markets.

Select components from the HiTest Template to configure a DIGITAL HiTest System. Any system configured as specified in the DIGITAL HiTest Template can be called a DIGITAL HiTest System.

Additional Hardware and Software

Besides the hardware and software specified in a DIGITAL HiTest Suite, additional hardware and software can be added to a HiTest System. Add-on hardware consists of accessory components such as printers, modems, and scanners that are supported by the operating system and other software. Adding these components should not affect interoperability and, therefore, the system can still be considered a DIGITAL HiTest System.

Customers who purchase a DIGITAL HiTest System that is configured below the maximum specified in the Template, can later add additional hardware up to the specified maximum range and still maintain the integrity of a DIGITAL HiTest System.

If additional hardware components beyond the maximum specified in the Template are configured into a system, you still have the assurance that the rest of the system has been thoroughly tested for component interoperability. Therefore, the risk of experiencing problems is greatly reduced.

2
About This DIGITAL HiTest Suite

This HiTest Suite satisfies the needs of customers who require a flexible and secure connection between their private network and the Internet, or other nonsecure public TCP/IP networks. It prevents unauthorized access to their private network, while providing controlled access to Internet services to users within their network.

AltaVista Firewall 97 is the only firewall that takes an active role in security management. With its unique intelligence, it warns of impending danger of intrusions, is constantly looking for threats to the defined security zone, and takes evasive action when attacks do occur.

AltaVista Firewall 97 combines trusted application gateways, comprehensive logging, reporting, real-time alarms, strong authentication, graphical user interface (GUI), and a step-by-step installation wizard all in one software package. AltaVista is by far the fastest firewall available, with no compromise on security. This demonstrates not only its high efficiency, but the tightness of its Windows NT integration.

Recognizing that users have platform and operating system preferences, DIGITAL offers AltaVista Firewall solutions on a choice of platforms running Windows NT. This HiTest Note describes the AlphaServer 800 platform. An AltaVista Firewall configuration on the Prioris MX is also available, described in AltaVista Firewall Windows NT Prioris MX DIGITAL HiTest Notes.

The AltaVista Firewall Windows NT AlphaServer 800 HiTest Suite includes the following components:

- AltaVista Firewall 97
- Windows NT Server 4.0
- AlphaServer 800

This chapter describes the following characteristics of the AltaVista Firewall Windows NT AlphaServer 800 HiTest Suite and evaluates the Suite in terms of each:

- Availability
- Installability
- Interoperability
- Manageability
- Price Range
- Scalability
- Services
- Year 2000 Compliance

Availability

Availability, which describes a computer system's ability to quickly recover from a failure, can be described in terms of the following:

- Data Protection – Ensures long-term data accessibility by providing the facility to do offline data backup.
- Data Availability – Stores redundant data on line for rapid, automatic data recovery in the event of a failure. Data availability is typically provided through the use of RAID technology.
- Platform Availability – Enables processing to continue during failure by using technologies that support failover to other components. Clustering, redundant power supplies, battery backup, and other components provide support for platform availability.
- Disaster Tolerance – Protects against computer room disasters such as fire, flood, and sabotage. Disaster Tolerant Systems require an additional system at a remote site and are more expensive than the previously defined alternatives. (The DIGITAL HiTest process does not test disaster tolerant configurations. If disaster tolerance is a requirement, your sales person can provide more information.)

Features of AltaVista Firewall Windows NT AlphaServer 800 HiTest Suite

This HiTest Suite is intended for those businesses where the unlikely failure of a hardware component is dealt with by service arrangement. Where the highest platform availability is a concern, DIGITAL recommends AltaVista High Availability Firewall System (order number DJ-WAMED-AA (U.S.A./Canada)) using a dual AlphaServer cluster.

Installability

Installability is the ease with which hardware and software components can be installed and configured for use. Factors that are considered when evaluating installability include clarity of installation steps, number of steps and duration appropriate to the complexity of the product, and completeness of the installation and configuration information.

The DIGITAL HiTest process thoroughly examined all aspects of the installation of this HiTest Suite. The installation procedures that were used are documented in Chapter 4. If these installation procedures are used, no problems should be encountered.

AltaVista Firewall 97 provides an installation wizard for easy step-by-step firewall installation, including Domain Name Server (DNS) configuration.

Within the HiTest environment, after removing the system from the shipping skid, it required two hours to install and configure the hardware for the maximum configuration and another four hours to install and configure the software, including the operating system. Expect installation times to vary significantly in other environments depending on factors such as the expertise of the installer and the environment in which the installation occurs.

DIGITAL Multivendor Computer Services (MCS) offers expert installation services.

Interoperability

Major components of this HiTest Suite have been tested for interoperability, including the application, operating system, hardware, firmware, and service packs and patches. Since interoperability problems are often related to inappropriate versions of components, the specific versions that are known to interoperate are documented. Minimum and maximum configurations for this Suite have been tested. The specific processes used for testing this Suite are described in Chapter 5.

The HiTest Notes provide solutions to interoperability problems in several ways. First, specific versions of all components are documented in Chapter 3. Second, installation and setup instructions in Chapter 4 are written so that many interoperability problems are avoided. Third, problems and solutions are documented in Chapter 6.

There are no major interoperability issues in this Suite.

Manageability

System manageability is the ease with which a system is managed or controlled. Because a system is composed of many components, manageability is described according to which component (application, database, operating system, server, storage, network) of the system is being controlled. For each of those components, manageability is measured by five features:

- Administration – The ease with which the systems management tools manage the system components
- Alarms – The effectiveness of triggers at detecting problems in system components
- Performance – The tuning and monitoring of system components
- Security – File access, user access, and intrusion detection
- Accounting – Logging the use of system resources

A firewall is a system that is connected to both the secure and the nonsecure network. A separate systems management station that is attached to a firewall can present a security risk. For this reason, Simple Network Management Protocol (SNMP) is disabled when AltaVista Firewall is installed. System management must be performed directly at the firewall system. It is also possible to perform remote administration of the firewall software using the Netscape browser with AltaVista Tunnel Personal Edition, which is shipped with the AltaVista Firewall software.

AltaVista Firewall 97 provides a comprehensive graphical user interface through which all configuration administration, and management tasks are performed.

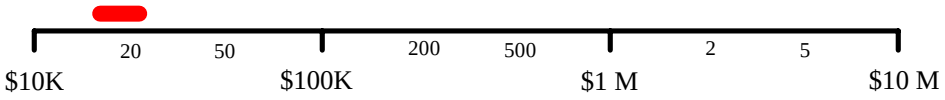
AltaVista Firewall 97 uses an active architecture that can take actions for the system administrator with a sophisticated alarming and notification system. Automatic alarms alert the system administrator to unusual or potentially threatening events relating to the firewall. The alarm system continually monitors the firewall system in real time for any events that are unusual or suspicious. Standard alarm actions include sending mail to the system administrator, raising the security status of the firewall, triggering a custom script and shutting down individual services or the entire firewall if the firewall is under continued or repeated attack. AltaVista Firewall for Windows NT can automatically shut down the service or the entire firewall to prevent the firewall from being compromised.

Price Range

Figure 2-1 shows the approximate list price (U.S. dollars) for the minimum and maximum HiTest Systems that can be configured from the AltaVista Firewall Windows NT AlphaServer 800 HiTest Suite. These prices were effective as of 1/20/98. The price range can vary significantly over time and with the inclusion of service packages, consulting, country-specific prices, and other factors.

The DIGITAL AlphaServer 800 system provides high performance at a competetive price for today's demanding applications. Systems configured from this HiTest Suite make a powerful yet affordable secure connection between the private network and nonsecure public TCP/IP networks.

Figure 2-1: AltaVista Firewall Windows NT AlphaServer 800 Price Range



The purchase price of a system is only one factor affecting affordability. The cost of staff, space, maintenance, and upgrade also affect the total cost of ownership. The system value is determined by comparing these costs to the total benefit and deriving the return on investment (ROI). Because these costs and the benefits are unique to each customer, the ROI can best be determined by a joint customer and sales person team.

Scalability

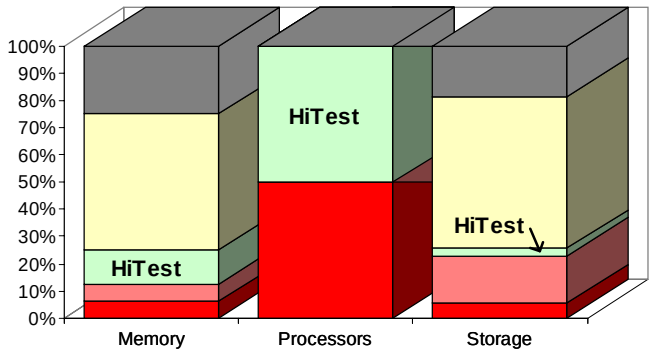
For this HiTest Suite, scalability can be described in two ways. In terms of hardware, scalability refers to the additional hardware components that can be added to a system within and beyond the HiTest configuration. In terms of performance, scalability refers to the workload capability of the HiTest configuration.

Additional Hardware Components

Systems that are configured from this HiTest Suite can easily be upgraded both within and beyond the ranges specified in the Suite.

In Figure 2-2, hardware scalability for this Suite is illustrated in terms of memory, number of CPUs, and disk space. Considering the limits imposed by the hardware enclosures in this HiTest Suite, Figure 2-2 shows the minimum and maximum limits of the system configuration. Table 2-1 provides the data from which this graph is derived.

Figure 2-2: AltaVista Firewall Windows NT AlphaServer 800 Scalability



Systems configured within this range involve tradeoffs between these, and sometimes other components.

Systems configured within this range generally exceed the requirements of the market.

HiTest — Systems configured within this range meet the requirements of most customers.

Systems configured within this range are generally insufficient to meet the requirements of the market.

Systems cannot be configured in this range.

Table 2-1: Scalability Data

Configuration	Memory	Processors	Storage
AlphaServer 800 Minimum	64 MB	1	2.1 GB
HiTest Minimum	128 MB	1	8.6 GB
HiTest Maximum	264 MB	1	8.6 GB
AlphaServer 800 Maximum (without tradeoff)	768 MB	1	29.4 GB
AlphaServer 800 Maximum Configurable	1,024 MB	1	36.4 GB

The AlphaServer 800 configurations of the AltaVista Firewall HiTest Suite meet the requirements of customers who require a flexible and secure connection between their private network and the Internet, or other nonsecure public TCP/IP networks. Significant expansion capability is provided for situations that may reach beyond the scope of this HiTest Suite.

In general, systems can be configured beyond the limits illustrated in Figure 2-2 by adding additional storage cabinets, clusters, and other peripherals.

Workload Capability

Scalability also measures how performance is affected as additional resources and users are added. When scalability is measured by workload capability, the factors that are considered include the effectiveness of additional hardware; whether the system remains consistent as you add to it; and how expensive it is to add to it.

DIGITAL HiTest Suites are selected to provide an appropriate workload capability for the target application area. Often a choice of suites is available, each providing appropriate coverage for specific situations. HiTest works closely with other DIGITAL groups to ensure that a HiTest system will perform appropriately in a production environment. Many HiTest systems are tested and tuned for performance.

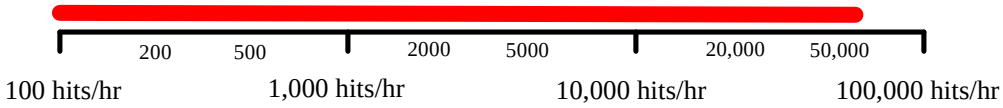
Characterization tests performed for Simple Mail Transfer Protocol (SMTP), FTP, and HTTP transactions showed that the AlphaServer 800 can handle up to 55,000 hits per hour. (A hit is defined as a single request from a web browser or other client for a single item from a web or other server.) The workload was tested on an AlphaServer 800 running Windows NT 4.0 with AltaVista Firewall 97. Three protocols were utilized: SMTP (send mail), HTTP (web content), and FTP (file transfer).

In today's business environment, most transactions take place through the SMTP or HTTP proxies. No problems were observed with either the SMTP or HTTP components in this configuration. Use of the FTP proxy includes essential security logging which may become a factor in situations where heavy FTP use occurs. (An FTP transaction using the FTP proxy is not the same as an FTP URL from within a web browser that uses a web proxy.) During FTP testing, this component had a significant impact and affected the disk requirements for the workload and the overall throughput of the server. Although FTP was less than 10% of the workload, FTP required substantial log files. When significant FTP use is predicted, additional disk space should be allowed. Regular inspection and removal of old FTP log files is recommended.

While our characterization tests showed that good performance can be obtained with memory near the minimum, prudence suggests use of additional memory when high workloads are expected.

Figure 2-3 shows the workload capability.

Figure 2-3: AltaVista Firewall Windows NT AlphaServer 800 Workload Capability



Services

DIGITAL offers a range of service options. The following portfolio of Business Critical Services is available for HiTest Suites and is backed by the DIGITAL Uptime Guarantee.

Proof of Commitment: The DIGITAL Uptime Guarantee

The DIGITAL Uptime Guarantee is a formal contract that commits DIGITAL to keeping a client's business critical systems in operation at least 99.5% of the time, excluding outages beyond the control of DIGITAL, such as electrical shutdowns, environmental failures, and downtime caused by application failure. If uptime levels are lower than 99.5%, clients do not pay the full service charge.

Portfolio of Business Critical Services

The three vital elements of DIGITAL Business Critical Services are:

- Availability Review

  The first step in initiating a Business Critical engagement with DIGITAL is a customized, in-depth availability analysis of the computing environment, beginning with an overview of operating goals. This review identifies potential risks and trouble spots in hardware, software, operations, physical environment, and network. A comprehensive written report forms the basis for determining serviceability requirements.

- Business Critical Gold Support

  Clients who purchase Business Critical Gold Support work with a named technical account manager who serves as the single point of contact and ensures that problems are resolved quickly. A privileged hotline assures crisis response within 30 minutes. An assigned support team works with the account manager to apply continuous effort to critical problems. The on-site support agreement for Gold Support Customers provides coverage 24 hours a day and seven days a week. Additional benefits include:

  – Notification of software patches as soon as they become available

  – Notification of known problems and fixes

  – Monthly service activity review

  – Operating system upgrade impact planning

  – Bi-annual System Healthcheck assessments. These are conducted using advanced system-based tools to assess the performance and security of systems. The collected data is analyzed against accepted practices, and the findings, together with recommendations for corrective action, are documented in a summary report.

- Availability Partnership

  With Availability Partnership, system availability is maintained at the required level by measuring and analyzing actual system availability, and conducting regular updates to the original Availability Review. Particular focus is placed on:

  – Configuration and topology documentation

- Availability status reporting
- Change impact analysis
- Proactive problem avoidance based on proactive patch/FCO/firmware management
- Periodic detailed data collection and analysis
- Availability model update
- Contingency planning
- Service planning and advising

Complementary Support Services

The three key Business Critical Services are augmented by:

- On-Site Parts Service

  DIGITAL works with the client to determine the appropriate inventory levels for their environment. A cost-effective *rental* parts solution is developed to maintain an on site inventory of spare parts.

- Installation and Startup

  DIGITAL offers rapid, worry-free implementation of new hardware and software – including systems, PCs, terminals, workstations, networking components, operating systems, layered products, applications, and software updates. Clients can choose hardware installation, software installation and startup, or both.

Meeting Client Needs Locally or Globally

With 450 service center locations in l00 countries, DIGITAL is prepared to deliver consistent and comprehensive service capabilities on a local or multinational basis. These services encompass:

- Total system support for servers, network operating system, applications, switching components, and PCs
- Multivendor support for a diverse range of products including networking equipment, applications, and peripherals
- Microsoft Solution Provider and Authorization Support Centers with the largest concentration of Microsoft certified engineers in the world

For More Information

To find out more about DIGITAL Business Critical Services, contact your local DIGITAL Multivendor Customer Services sales specialist or visit the Business Critical Services web site at `http://www.digital.com/services/mcs/mcs_critical.htm`.

Year 2000 Compliance

Year 2000 Compliance refers to whether computer systems will properly recognize the date change from December 31, 1999 to January 1, 2000. Current information on Year 2000 status of DIGITAL products can be obtained from the DIGITAL Year 2000 Program web site at `http://ww1.digital.com/year2000/`. Current information on the Year 2000 status of other vendor's products should be confirmed with those vendors.

While HiTest does not explicitly test for year 2000 compliance in the components of this Suite, HiTest does check the published status of components where Year 2000 compliance would be a concern. Table 2-2 summarizes these findings.

The color codes used in the table represent the following categories of readiness:

- Blue – Version specified is Year 2000 ready today.
- Green – Currently not Year 2000 ready. Version to be Year 2000 ready specified with Year 2000 date noted.
- Yellow – Under evaluation.
- Red – Will not be made Ready for Year 2000. Product will be removed from active status on or before 31 March 1998.
- N – Not Applicable - No Year 2000 implications exist for this component.

Table 2-2 shows the AltaVista Firewall NT AlphaServer 800 Year 2000 Compliance status.

Table 2-2: AltaVista Firewall Windows NT AlphaServer 800 Year 2000 Compliance

Component	Year 2000 Status
AltaVista Firewall 97	Green
Windows NT Server	Blue
AlphaServer 800	Blue

AltaVista Firewall 97 is not considered Year 2000 compliant. AltaVista Firewall 98 provides Year 2000 compliance.

3
Configuration Data

This chapter describes theAltaVista Firewall Windows NT AlphaServer 800 DIGITAL HiTest Suite including the hardware, software, and firmware components and their revision levels. If required, special configuration rules are explained.

Hardware and Software Components

Table 3-1 and Table 3-2 identify the range of hardware and software components that can be configured using the AltaVista Firewall Windows NT AlphaServer 800 HiTest Suite. These two tables form the DIGITAL HiTest Template. The ranges of hardware provided in this template include 128 MB through 256 MB of memory, one 4.3 GB disk, and two Fast Ethernet or FDDI controllers.

Table 3-3 lists the revision levels of the components.

The DIGITAL HiTest Template consists of three categories:

- AppSet Software – Includes software specific to one class of customer solutions, in this case AltaVista Firewall 97
- Foundation Hardware – Includes the base system, storage, and other hardware options
- Foundation Software – Consists of the operating system software

When ordering an item from a HiTest Template, select a quantity that is within the minimum and maximum range for the item. If the minimum quantity is zero (0), then the component is optional. If the minimum quantity is one or more, order at least the minimum quantity, but be cautious about exceeding the maximum quantity. The maximum quantity represents the greatest number of components that were tested for interoperability with all the other components in the Suite.

For more details on the HiTest Suite hardware configuration, see Chapter 7.

Table 3-1: DIGITAL HiTest Template – AppSet Software and Foundation Hardware

AltaVista Firewall HiTest AppSet Windows NT AlphaServer 800 HiTest Foundation Hardware				
For documentation and updates: http://cosmo.tay.dec.com and http://www.partner.digital.com:9003/cgi-bin/comet				
Line Item	**Description**	**Part Number**	**HiTest Range**	
			Min	**Max**
AppSet Software				
1	*Select one of the following:* **AltaVista Firewall 97, NT Alpha, 25 Nodes, Lic & CD** **AltaVista Firewall 97, NT Alpha, 50 Nodes, Lic & CD** **AltaVista Firewall 97, NT Alpha, 200 Nodes, Lic & CD** **AltaVista Firewall 97, NT Alpha, Unlimited Nodes, Lic & CD** **Note:** AltaVistaFirewall 97 includes AltaVista Tunnel Personal Edition. This AppSet is not required when the foundation hardware and software is ordered for use with a non-HiTest application.	 **QB-55YAA-SH** **QB-55YAA-SB** **QB-55YAA-SC** **QB-55YAA-SD**	1	1
Foundation Hardware				
2	*Select one base system:* **AlphaServer 800 5/400 System, Pedestal, 128 MB** **AlphaServer 800 5/400 System, Rackmount, 128 MB** *Hardware includes*: • CPU with 2 MB cache • 128 MB memory • S3 SVGA integrated Graphics • DE500-AA 10/100 Mbit Fast Ethernet • Qlogic ISP1020 Integrated SCSI controller and cable • SCSI 12X CD-ROM drive • RX23L-AB 1.44 MB Floppy drive • 4.3 GB UltraSCSI disk (RZ1CB-SB) **Note:** Systems ordered in the Americas or Asia Pacific include the keyboard. *Software includes*: • Windows NT Server 4.0 operating system • 10-client access license and media	 **PB81B-AN** **PB81P-AN**	1	1
3	**64 MB Memory Option** **128 MB Memory Option** **Note:** This HiTest template supports a memory range from 128 MB to 256 MB. When selecting memory options, stay within the template's 256 MB maximum.	**PB8MA-AC** **PB8MA-AD**	0	See Note
4	**4.3 GB 7200 RPM UltraWide SCSI Disk Drive**	**RZ1CB-SB**	1	1
This HiTest Suite requires two network adapters. Select either an Ethernet Adapter (lines 5 and 6) or FDDI Adapters (lines 7 and 8).				
Ethernet Adapter				
5	*Order one 10/100 adapter:* **Fast EtherWORKS PCI 10/100 NIC**	**DE500-AA**	1	1
6	*Order one cable for each 10/100 adapter:* **10BaseT Twisted-Pair Ethernet cable**	**BN25G-07**	2	2
FDDI Adapter				
7	*Order two FDDI adapters:* **PCI to FDDI adapter SAS, MMF, SC**	**DEFPA-AB**	2	2

AltaVista Firewall HiTest AppSet Windows NT AlphaServer 800 HiTest Foundation Hardware				
For documentation and updates: http://cosmo.tay.dec.com and http://www.partner.digital.com:9003/cgi-bin/comet				
Line Item	**Description**	**Part Number**	**HiTest Range**	
			Min	**Max**
8	*Order one cable for each FDDI adapter:* **20-m SC to SC dual fiber-optic cable**	**BN34B-20**	2	2
9	*Select one high-resolution color monitor:* **15-in Flat-square with 0.28 dot pitch** **17-in Trinitron aperture grille, 0.25mm** **21-in Diamondtron aperture grille, 0.28 dot pitch**	**SN-VRCX5-WA**ⓘ **SN-VRTX7-WA**ⓘ **SN-VRCX1-WA**ⓘ	1	1
ⓘ Indicates that geography-specific part number variants are available. Check the appropriate price book for details.				

Table 3-2: DIGITAL HiTest Template – Foundation Software

Windows NT AlphaServer 800 HiTest Foundation Software						
For documentation and updates: http://cosmo.tay.dec.com and http://www.partner.digital.com:9003/cgi-bin/comet						
Line Item	**Description**	**Part Number**	**HiTest Range**		**Required By**	
			Min	**Max**	**Fnd**†	**App**†
Foundation Software						
1	**Windows NT Server 4.0**	**Included with item 2 of Table 3-1**	1	1	Yes	Yes

2	**Windows NT Server Service Pack 3**
	Contact Microsoft at:
	`http://www.microsoft.com`
	or (800) 360-7561, or download from:
	`ftp://ftp.microsoft.com/bussys/winnt`
		Microsoft	1	1	Yes	Yes

3	**Hard copy of this Suite's HiTest Notes**	**EK-HAFNF-HN**	1	1	Yes	Yes
†Fnd = Foundation, App = AppSet						

Table 3-3: Component Revision Levels

Hardware Component	Hardware	Firmware	Software
5/400 MHz CPU	D02	–	–
4.3 GB disk (RZ1CB-SB)	–	DEC LYJ0	–
Fast Ethernet Controller (DE500-AA)	B01	1.1	–
SRM Console	–	5.0-104	–
AlphaBIOS	–	5.30	–
CD (RRD46)	–	0557	–
Software Component		**Version/Revision**	**Patch Level**
Windows NT Server		4.0 (Build 1381)	Service Pack 3 (SP3)
AltaVista Firewall 97		3.0 (970301)	–
AltaVista Tunnel 97 Personal Edition		3.0	–
SMTPXD.EXE		1.0-1	–

Special Configuration Rules

When configuring the AltaVista Firewall Windows NT AlphaServer 800, it is possible to order more or less memory than is supported by the DIGITAL HiTest Templates. To comply with the HiTest Template, keep the total installed between 128 MB and 256 MB.

The *AlphaServer 800 Owner's Guide* provides configuration information needed to properly install memory and PCI options.

See the *AlphaServer 800 Technical Summary* for a description of the system including hardware components, server management, and maintenance.

4
System Installation and Setup

This chapter describes how to install and set up a DIGITAL HiTest System configured from this DIGITAL HiTest Suite. System preparation includes installing hardware, the operating system, and applications.

The following topics are covered in this chapter:

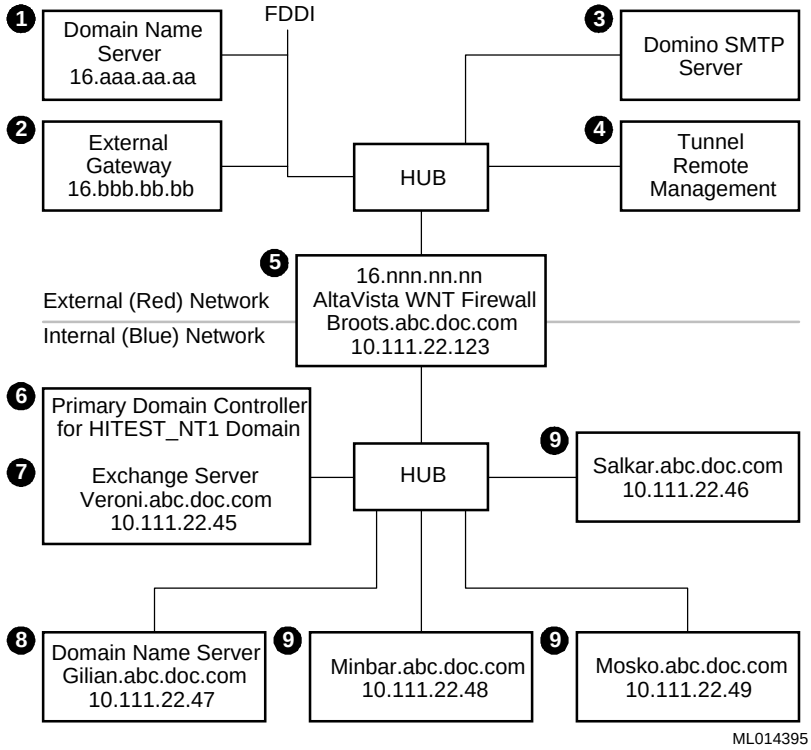
- Understanding the Firewall Environment – An overview of configuration considerations for a firewall environment.
- Summary of Installation Tasks – A high-level description of the tasks involved in setting up a firewall environment.
- HiTest Case Study – A detailed description of how the HiTest environment was built. The HiTest case study is offered to help clarify installation concepts; it may or may not apply to your site.

Understanding the Firewall Environment

Before installing the AltaVista Firewall server hardware and software, it is necessary to determine how your the firewall environment will be structured. This includes the external (red) network, the firewall system, and the internal (blue) network.

Figure 4-1 provides a high-level view of a firewall configuration, illustrating the aspects of each part of the network that should be considered. This figure is used throughout the chapter to illustrate configuration steps. Chapter 5 provides a detailed description of the HiTest environment, which may also be useful when configuring your firewall.

Figure 4-1: Firewall Environment



Configuration considerations for the external (red) network:

❶ The external Domain Name Service (DNS) server must know that the firewall server is authoritative for the firewall domain.

❷ An external gateway allows connection to an external network such as the Internet. If the firewall system is connected to an external gateway, you must obtain a registered external network address for the firewall adapter.

❸ If you want a mail gateway to the firewall, configure an external server to route external mail to the firewall.

❹ While SNMP-based system management is not possible, the configuration of the AltaVista Firewall itself may be remotely administered using the Netscape browser with the AltaVista Tunnel Personal Edition (provided with the AltaVista Firewall software).

Configuration considerations for the firewall server:

❺ The network interface cards in the firewall server must be configured with TCP/IP. One of these is connected to and configured for the external gateway, using a registered IP address. The second adapter is connected to the internal network. DIGITAL recommends that the internal adapter be configured for hidden DNS for security reasons. This also allows the use of unregistered IP addresses inside the firewall.

Configuration considerations for the internal (blue) network:

❻ The primary domain controller must be a server other than the firewall server.

❼ The internal mail server becomes the mail hub that forwards all outgoing mail to the firewall server and receives all incoming mail.

❽ One or more DNS servers are required for the internal network. Having more than one DNS server allows for failover. One name server must be selected as the primary name server, which will be the authoritative name server for all internal hosts in the domain.

❾ All servers in the internal network must be registered on the DNS server.

Summary of Installation Tasks

This section provides a high-level summary of the tasks that must be performed to set up the firewall system, including:

- Preparing the Firewall Environment
- Hardware Installation Overview
- Windows NT Server Installation Overview
- AltaVista Firewall 97 Installation Overview
- Postinstallation Configuration Overview

Details of completing these tasks are provided in the HiTest case study later in this chapter.

Preparing the Firewall Environment

The following list summarizes the tasks that should be performed to prepare the firewall environment:

1. Become familiar with the *AltaVista Firewall 97 Installation Guide* and the *AltaVista Firewall 97 Administrator's Guide.*
2. Answer the following questions:
   - Will name resolution be with open or hidden DNS?
   - Will internal IP addresses be registered?
   - Is a mail server required inside the firewall?
   - Will authentication be by Hand Held Authenticator (HHA) or NT Domain?
   - Which proxies will be used: Finger, FTP, Web, RealAudio, SMTP, SQL *Net, Telnet, News, Generic TCP
   - What access levels are required for the various proxies?
3. Record the IP addresses that are needed for the firewall internal and external network adapters.
4. Configure one or more DNS servers for the internal network.
5. If present, configure the internal mail server with an SMTP connector and set it to forward to the firewall.

Hardware Installation Overview

The following list summarizes hardware installation tasks:

1. On the firewall server, connect a network cable to the NT network adapter that will be used for the internal network.
2. After installing Windows NT server, connect the firewall external network adapter to the external network.

Windows NT Server Installation Overview

The following list summarizes the tasks to install Windows NT server:

1. Install Windows NT Server on the firewall server and select TCP/IP as the network protocol. Do not make the firewall a domain controller.
2. Assign IP addresses to each network adapter.
3. Join the server to an NT domain in the internal network.

AltaVista Firewall 97 Installation Overview

The following list summarizes AltaVista Firewall installation tasks:

1. Insert the AltaVista Firewall 97 software CD and run setup.
2. If remote management is desired, select this option when prompted.
3. Select the external IP address when prompted.
4. Select open or hidden DNS when prompted.
5. Enter DNS and Mail Server information when prompted.

Postinstallation Configuration Overview

The following list summarizes postinstallation configuration procedures:

1. Configure the firewall's authentication service so that authorized users are granted access.
   - If NT Domain authentication is used, specify the domain name under the authentication tab of the AltaVista Firewall manager.
   - If Hand Held Authenticators (HHAs) are used, configure them according to AltaVista documentation.
2. If remote management was installed, configure one or more tunnels using the instructions in the *AltaVista Firewall 97 Administrator's Guide*.
3. If web browsers are used in the internal network, configure them to use the firewall as a proxy.
4. Configure individual proxies as needed and stop proxies that are not being used.
5. Test individual proxies. (See chapter 5 of this HiTest Note.)
6. Test remote management. (See chapter 5 of this HiTest Note.)

HiTest Case Study

The following procedures describe the installation processes used to set up the AltaVista Firewall Windows NT AlphaServer 800 HiTest configuration. They represent one of several ways to setup the firewall and may or may not apply to your site. Use the procedures as an aid to help clarify installation concepts.

Preparing the Firewall Environment

Several aspects of the existing network should be configured before you begin installing hardware and software on the firewall system. These include:

- Configuring DNS and mail for the internal network
- Configuring the internal mail server

Configuring DNS and Mail for the Internal Network

DNS is the host and lookup service for the Internet network. You can set up DNS on the firewall in either an Open or Hidden configuration. In an Open DNS configuration, the firewall system provides information about hosts on the internal network in response to requests from external or internal hosts.

With a Hidden name service, the firewall system provides information only about the system itself and its aliases. Information about hosts on the internal network is hidden from the external network. DIGITAL recommends a hidden name service for firewall systems.

Before installing the firewall system, you must configure the internal DNS server which provides the host and lookup service for the internal network. While the internal network may be a new network being configured for the first time, a firewall can be placed between two previously unseparated networks. When this is done, it is recommended that you readdress the internal hosts by assigning unallocated addresses in the format 10.a.b.c. It is also recommended that you create a new domain for the internal network to make it clear which hosts are internal.

To configure DNS on an internal name server:

1. Log in (with administrative privileges) to the internal server which will act as the DNS server.
2. From the Control Panel, display Network Services and Add a Microsoft DNS Server.
3. When prompted, use the Windows NT server installation CD-ROM to install the Domain Name Service.
4. Run the DNS Manager. The Domain Name Service Manager dialog box is displayed.
5. Create a new server record:
    a. Pull down the DNS menu and choose New Server. The Add DNS Server dialog box displays.
    b. Enter the IP address of the server, and click OK. The address is displayed in the left panel.
5. Create a new zone record:
    a. Pull down the DNS menu and choose New Zone. The New Zone dialog box displays.
    b. Enter the name of the internal DNS domain, for example `abc.doc.com`.
    c. Click OK. The Name Server (NS) and Start of Authority (SOA) records are created and the domain name is displayed in the left panel.

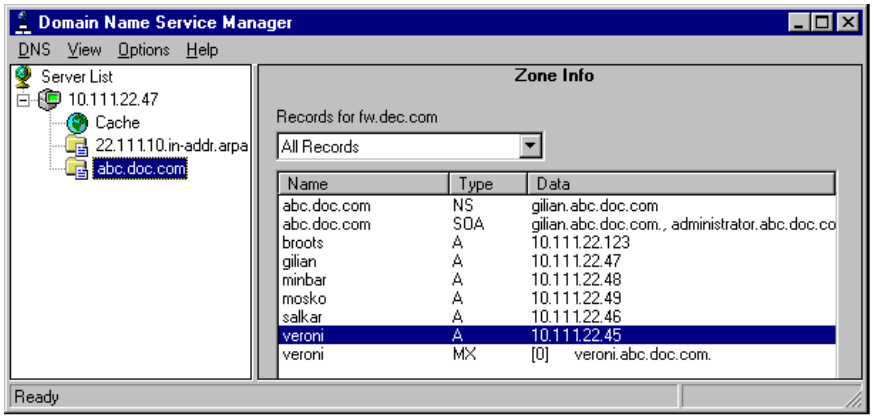
6. Create a DNS reverse zone in the In-addr.arpa domain. This is used to store the reverse lookup (PTR) records.
   a. Select the IP address of the name server, right click, and choose New Zone.
   b. Under Zone Type, click the Primary radio button.
   c. Enter the zone name. Use the following format:

      nn.nnn.nn`.in-addr.arpa`

      where *nn.nnn.nn* is the network portion of the name server IP address in reverse order. For example, if the IP address is 10.111.22.47, the zone name is `22.111.10.in-addr.arpa`.
   d. Enter the zone file name, which is the same as the zone name with the extension `.dns`. For example, `22.111.10.in-addr.arpa.dns`.
7. Create new records for each host in the domain:
   a. Select the domain name in the left panel.
   b. Pull down the DNS menu and choose New Host.
   c. Enter the host name and IP address.
   d. Click the "Create Associated PTR Record" radio button. This stores the reverse lookup record in the primary zone you created in step 6.
8. Create an MX record for the internal mail server:
   a. Select the domain name in the left panel.
   b. Pull down the DNS menu and choose New Record.
   c. Under Record type, choose MX record.
   d. In the Host Name field, enter an alias if desired.
   e. In the Mail Exchange Server DNS Name field, enter the fully qualified domain name, for example `veroni.abc.doc.com`.
   f. Enter a number in the Preference number field. This field determines the forwarding order when more than one mail server is configured for a domain. The highest preference is 0.

Figure 4-2 illustrates the Domain Name Service user interface and shows records which correspond to the internal network illustrated in Figure 4-1.

Figure 4-2: Domain Name Service Manager



9. Set forwarders to point to the firewall system so that any DNS queries that are not satisfied by the internal DNS are forwarded:
    a. In the Server List, select the IP address, right click, and choose Properties.
    b. In the Server Properties dialog box, click the Forwarders tab.
    c. Click the "Use Forwarders" and "Operate as a Slave Server" check boxes.
    d. Select the address of the firewall server, and click Add.

Configuring the Internal Mail Server

The firewall uses SMTP proxy to provide access between the external network and systems on the internal network. The mail server should be configured with an SMTP connector. HiTest used Microsoft Exchange which was configured as follows:

1. Run the Microsoft Exchange Administrator on the Exchange server for the internal network.
2. Pull down the File menu, choose New Other, then choose Internet Mail Service.
3. Double click the server to be configured with SMTP, then click the Connections tab.
4. Under Message Delivery, click the "Forward all messages to host" radio button and enter the IP address of the firewall server. Other options are available on this screen; the HiTest environment used the defaults.

Hardware Installation

The *AlphaServer 800 Owner's Guide* provides instructions for installing your AlphaServer 800 system. Chapter 7 in this HiTest Note provides additional information specific to the minimum and maximum configurations of this HiTest Suite.

If you use Hidden DNS and configure unregistered IP addresses for the hosts in the internal (blue) network, use caution when connecting the network adapters. Ping the cards to verify which is the internal network.

It is recommended that you connect the network adapter to the external network after installing and configuring Windows NT Server.

Operating System Installation

This section describes how to install the Windows NT Server operating system, including Service Pack 3 (SP3).

Windows NT Server Installation

The AlphaServer 800 comes with the Windows NT Server operating system already installed. When configuring your system, refer to the *Microsoft Windows NT Server Start Here (Basics and Installation)* book, provided with your server software.

To configure your system:

1. Make sure you have the following information, required to complete your configuration:
    - Product key – 20-digit number that appears on your certificate of authenticity

      or CD Key – 10-digit number that appears on the CD case
    - Unique name – to identify your computer on the network
    - NT domain name
    - Internal and external IP addresses
2. Boot the system. The configuration screen displays.

3. Choose the “Typical” setup option and follow the prompts to configure the system. Use the defaults and provide the required information when prompted.
4. When prompted to choose a server type, choose Standalone.
5. Configure the firewall server to connect to the Network. You can also install or modify your network connections after Setup is complete by double clicking Network in the Control Panel.
   a. When prompted to install IIS, do not select it. If you choose to install remote management, IIS is installed by the firewall install wizard at that time.
   b. Setup automatically detects the adapters installed in the firewall server.
   c. When prompted, choose TCP/IP as the network protocol.
   d. Configure the TCP/IP properties for both the internal and external network adapters shown in Table 4-1. The examples shown correspond to the information in Figure 4-1.

Table 4-1: TCP/IP Setup

Property	Description	Example
Internal network - PCI Fast Ethernet card 1		
IP Address	IP address for the internal network card	10.111.22.123
Subnet Mask	Internal subnet mask	255.255.255.0
Default Gateway	None	None
External network – PCI Fast Ethernet card 2		
IP Address	Registered IP address for the external network card	16.nnn.nn.nn
Subnet Mask	External subnet mask	255.255.252.0
Default Gateway	Registered IP address of external gateway server	16.bbb.bb.bb
DNS		
Host Name	Name of firewall server	broots
Domain	Name of the NT domain	HITEST_NT1
DNS Service Search order	IP address of the primary DNS server in the internal network	10.111.22.47
DHCP	Dynamic Host Control Protocol (optional)	not used
WINS	Windows Internet Naming Service (can be used instead of DNS)	not used

When you finish configuring the network, Windows NT tries to connect you to the Primary Domain Controller. The ability to make that connection confirms the success of the Windows NT Server installation.

If the Windows NT Server operating system is not installed, or if you need to reinstall Windows NT Server, complete the following procedure:

1. Make sure you have the information in step 1 of the previous procedure.
2. Load the Windows NT Server 4.0 CD-ROM into the CD drive.

3. From AlphaBIOS Setup, select “Install Windows NT,” and press Enter.
4. Complete steps 3 through 5 in the previous procedure.

Service Pack Installation

Service Packs are available from the following sources:

- A Microsoft reseller
- The Microsoft web page at: `http://www.microsoft.com`
- The Microsoft Order Desk in the United States at (800) 360-7561 between 6:30 A.M. and 5:30 P.M., Pacific time
- The Microsoft ftp support site located at: `ftp://ftp.microsoft.com/bussys/winnt`

Install Windows NT Service Pack 3 (SP3).

Note

Windows NT Service Pack 3 (SP3) *must* also be re-installed after installing any applications.

AltaVista Firewall 97 Installation

This section describes how to install and configure the AltaVista Firewall software on the AlphaServer 800 system. It also describes postinstallation tasks including user authentication setup and remote firewall administration.

To install AltaVista Firewall 97:

1. Before installing the AltaVista Firewall software, have the following available:
   - The *AltaVista Firewall 97 Installation Guide*, provided with your AltaVista Firewall software
   - The Windows NT Server CD-ROM, required to install the Internet Information Server (IIS)
2. Insert the AltaVista Firewall CD-ROM into your CD-ROM drive.
3. Run `X:\alpha\setup`, where X is the letter of your CD-ROM drive.
4. Select “Remote Management.” Remote management allows you to securely manage your firewall from a location other than the firewall system.
5. When prompted, insert the Windows NT Server CD-ROM and follow the instructions to install IIS. When you finish installing IIS, the AltaVista Firewall Network installation screen displays.
6. On the Network installation screen, click the radio button for the card that connects to the external network.
7. Click the “Set internal network list” button, then click Next. The Internal Network List dialog box displays, with the internal IP address and subnet mask you have specified for the firewall system.

   If necessary, you can change the address or add additional addresses for multiple subnets. You can also add and modify these addresses after installation.
8. Click OK. The Configure DNS dialog box displays, with the NT domain name and firewall host name you defined for TCP/IP during the Windows NT installation.

9. Click the “Hidden DNS” radio button.
10. Set the rest of the DNS parameters shown in Table 4-2. These parameters correspond to the parameters you configured on the internal DNS server. The examples shown for the match the values in Figure 4-1.

Table 4-2: AltaVista Firewall DNS Parameters

DNS Parameter	Description	Example
Domain Name	DNS domain name	abc.doc.com
Name of Firewall Host	Name of Firewall system	broots
Internal Name Server Name	Fully qualified name of internal DNS Server	gilian.abc.doc.com
Internal Name Server Address	IP address of internal DNS server	10.111.22.47
External Name Server Name	Name of external DNS server (or address of external DNS server)	16.aaa.aa.aa
Internal Mail Hub Name	Fully qualified name of internal mail server	veroni.abc.doc.com

11. Obtain the latest SMTP proxy driver (SMTPXD.EXE) from the AltaVista Software web site at:

    `http://AltaVista.software.Digital.com/`

    This new driver has enhancements for SMTP operation. Copy the new SMTPXD.EXE daemon to the `dfw\bin` directory. Set the NT registry value as desired, following the instructions in the readme file that comes with the patch.

12. Re-install Windows NT Service Pack 3 (SP3).

Postinstallation Tasks

After AltaVista Firewall is installed and configured, you can perform many postinstallation configurations using the AltaVista Firewall management user interface. Determine the configurations required for your environment using the *AltaVista Firewall 97 Administrator’s Guide*.

This section describes User Authentication Set Up and Remote Firewall Administration Set Up, both of which are recommended for systems configured from this HiTest Suite.

User Authentication Set Up

For FTP or telnet proxies, you can choose security policies that grant certain types of access only to users who can authenticate their identity. If you choose such policies, you must configure the firewall’s authentication service so that the required users are granted access. AltaVista Firewall provides two types of authentication: NT Domain authentication or the use of Hand Held Authenticators (HHA). See the *AltaVista Firewall 97 Administrator’s Guide* for a description of how to configure HHA.

NT Domain authentication is described in the following procedure. In this form of authentication, users are given logon privileges to a domain rather than to each individual server. Once logged on to the domain, users can access resources for which they have been granted privileges.

To configure authentication for the NT Domain:

1. Run the AltaVista Firewall Manager.

2. Choose the Authen tab. The system displays the Authentication Services dialog box.
3. Click the "Authentication in the NT domain" radio button and enter the domain name in the edit field. The firewall system was configured to be part of the domain when TCP/IP properties were set as part of the Windows NT installation.

Note

The firewall GUI does not allow the use of domain names containing underscores. To work around this restriction, enter the domain name without the underscores, then modify it in the registry to add the underscores:

1. Run `regedit`.
2. Go to HKEY_LOCAL_MACHINES\SOFTWARE\Digital Equipment Corporation\Firewall\
3. Modify the AuthDomain property to add the underscore.

Remote Firewall Administration

The AltaVista Firewall uses the AltaVista Tunnel server software to implement remote management channels. Each of these channels is based on a tunnel that is set up between the firewall and the remote host. When a tunnel is started, the AltaVista Tunnel software authenticates the firewall and the remote host.

Note

A modified version of AltaVista Tunnel, AltaVista Tunnel Personal Edition, is included with AltaVista Firewall. This version of AltaVista Tunnel allows you to set up as many remote management channels as you want, but you can only run one remote management session at a time.

Before setting up remote firewall administration, make sure you have installed the Remote Administration Option when you installed the AltaVista Firewall. In addition, remote firewall administration using AltaVista Tunnel based on the use of a web browser and requires that Netscape be installed.

Creating a Remote Management Channel

When you create a remote management channel, you create an encryption key that protects the security of the firewall and assigns a username and password for use when making the connection from the remote client to the firewall.

To add a remote management channel to the local firewall host:

1. Log in to the firewall system and run the AltaVista Firewall Manager.
2. Select the Remote tab.
3. Under "Add Remote Channel," enter the parameters shown in Table 4-3. The IP addresses required are used only by the tunnel. AltaVista recommends that you use RFC 1918 private addresses such as those shown in the table. Do not use real addresses from your network.

Table 4-3: Remote Channel Parameters

Parameter	Description	Example
Channel Name	Unique one word name for this tunnel. This will be the username for the tunnel client.	Abcmanager
Firewall Virtual Address	A unique IP address for the firewall system.	192.168.1.204
Client Virtual Address	A unique IP address for the client system.	192.168.1.205
Network Mask	The subnet mask of the internal network.	255.255.255.0

4. Click Add. A password dialog box displays.
5. Enter and confirm the password to be used by the tunnel client to login.
6. Extract the crypto key for use by the tunnel client:
   a. Select the channel you just added.
   b. Click Extract Key to create the `.eta` and `.key` files for the tunnel. By default these files use the tunnel name you specified.
   c. Save the files to a floppy diskette and label it. Use this diskette to transport the files to the remote client.

AltaVista Tunnel Client Installation and Configuration

The AltaVista Tunnel client software is installed on the remote host (workstation or server) from which the firewall will be managed.

To install the AltaVista Tunnel client on a remote system running Windows NT:

1. Insert the AltaVista Tunnel Personal Edition software diskette in the floppy drive.
2. Display the control panel and double click Network.
3. Select the Services tab.
4. Click Add, then click the “Have Disk…” button.
5. Navigate to the drive containing the AltaVista Tunnel software and select the AltaVista Tunnel Service file.
6. Click OK. The service is installed.

For instructions on how to start a tunnel session and use the remote host to manage a firewall, see the Firewall Administration section of Chapter 5.

Proxy Configuration

AltaVista Firewall uses trusted proxies to connect users in your internal network to the external network. The firewall uses proxies for all services that requires a connection. The following proxies are installed on the firewall system when you install the firewall software:

- World Wide Web (Web)
- FTP
- Telnet
- SMTP
- News
- RealAudio

- Generic (for custom applications)
- SQL*Net
- Finger

With proxies, users do not connect directly to services; instead, they connect to a proxy on the firewall system. If the connection is permitted, the proxy relays the request to the appropriate destination.

In addition to proxies for specific services, you can create generic proxies and configure them to your requirements. This allows you to control connections to services such as tunnel for which individual proxies are not provided.

After you install the firewall for the first time, it is active but allows connection only to web proxy and mail proxy services. To use other proxies, you must specify the security policies you want to use.

To configure proxies:

1. Run AltaVista Firewall management and choose the Services tab.
2. If the service you want to configure is running, select it and click Stop.
3. Click Setup to display the Setup Proxies dialog box.
4. Choose the tab of the proxy you want to configure.
5. Configure the proxy using the instructions in the chapter on configuring NT proxies in the *AltaVista Firewall 97 Administrator's Guide*.

You should also stop any proxies that you do not plan to use.

5
Tests and Results

The DIGITAL HiTest program tests for several types of problems that affect the system. The HiTest program works together with other organizations to obtain and share test information for other categories.

This chapter describes the overview of test results, how the tests were set up, and where the data and programs were placed.

Also covered in this chapter is the test environment, tools used for testing, test configuration, test management, and the test process.

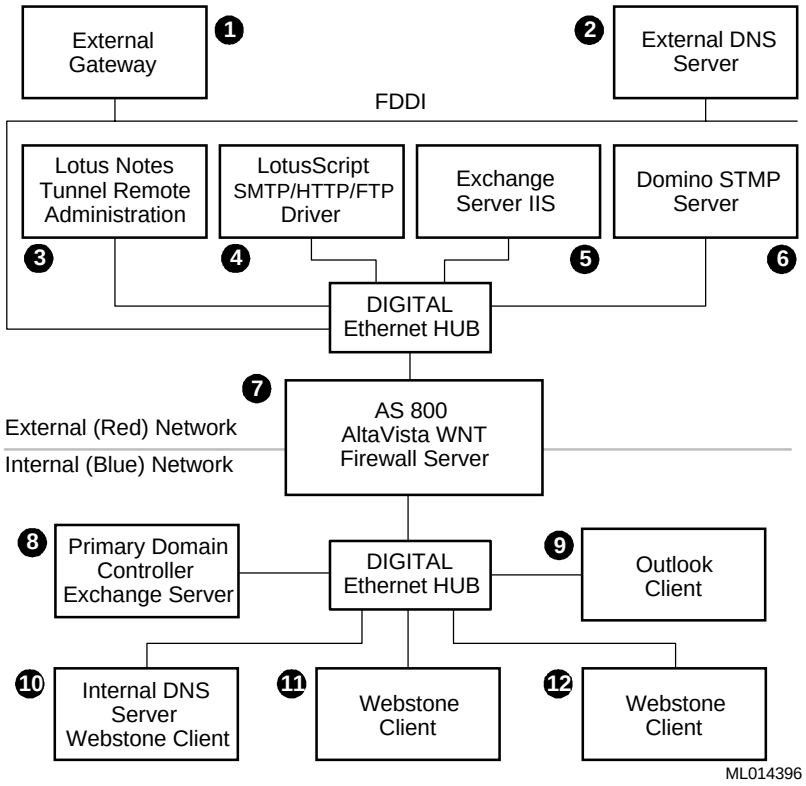
Overview of Results

Interoperability testing was performed successfully on the AltaVista Firewall Windows NT AlphaServer 800 HiTest Suite. Tests were performed to ensure the suite met installability and interoperability criteria. Workload characterization was also performed.

Test Environment

Figure 5-1 shows the AltaVista Firewall Windows NT AlphaServer 800 test environment.

Figure 5-1: Test Environment



1. External Gateway server
2. External Domain Name Server (DNS)
3. Lotus Notes and Tunnel Remote Administration by way of Netscape
4. LotusScript and SMTP/HTTP/FTP drivers: performed automated SMTP/HTTP/FTP operations
5. External Exchange Server and Internet Information Server (IIS)
6. External Lotus Domino and SMTP Server
7. AlphaServer 800 HiTest AltaVista Firewall Server
8. Primary Domain Controller for HITEST_NT1 domain and internal Exchange server
9. Outlook Client: sent mail to external (red) network
10. Internal DNS Server and Webstone Client: received web pages from external IIS Server
11. Webstone Client: received web pages from external IIS Server
12. Webstone Client

Test Tools

The following tools were used to test interoperability:

- Webstone to perform web browsing HTTP testing
- Manual demonstrations of alarms

- Custom LotusScript to perform web browsing, FTP, and SMTP operations across the firewall
- Manual demonstrations of FTP and Telnet

Test Load

The test load generated for interoperability testing was as follows:

- Webstone tests were run with a throughput of between 270 and 300 pages per minute
- The mail/HTTP processing test duration was 40 hours
- Testing exercised the following functions across the firewall:
  - Get web pages from external IIS server
  - Get web pages from internal IIS server
  - FTP to external and internal servers
  - Telnet to external and internal servers
  - Use automated scripts to send mail across the firewall in both directions
  - Configure proxies to disallow external and internal access and verify that access is denied and alarms function

Tests were run concurrently in each 40 hour test period. For mail and the HTTP web, multiple concurrent sessions were run against each relay.

Test Configuration

This section describes the disk configuration of the HiTest test environment. HiTest tested a disk configuration greater than the configuration recommended in the HiTest Templates in Chapter 3. As a result of that testing, it was determined that two disks should be the maximum recommendation for this HiTest Suite.

Minimum Configuration

The minimum configuration included two UltraSCSI disks connected to an integrated SCSI controller, as shown in Table 5-1.

Table 5-1: Disk Configuration for the Minimum Configuration

Disk Drive Group Name	Number of Disk Drives	Disk Drive Locations	Disk Drive Content and Data	Group Type	Usable Capacity
C:	1	Drive 1 – SCSI ID 0	Windows NT system and paging file	JBOD	4.3 GB
D:	1	Drive 2 – SCSI ID 1	AltaVista Firewall 97, AltaVista Tunnel, file shares, and log files	JBOD	4.3 GB
					Usable Total: **8.6 GB**

Maximum Configuration

The maximum configuration tested included four UltraSCSI disks connected to an internal SCSI controller, as shown in Table 5-2.

Table 5-2: Disk Configuration for the Maximum Configuration

Disk Drive Group Name	Number of Disk Drives	Disk Drive Locations	Disk Drive Content and Data	Group Type	Usable Capacity
C:	1	Drive 1 –SCSI ID 0	Windows NT system and paging file	JBOD	4.3 GB
K:	3	Drive 2 – SCSI ID 1 Drive 3 – SCSI ID 1 Drive 4 – SCSI ID 1	AltaVista Firewall 97, AltaVista Tunnel, file shares, and log files	NT striping with parity (RAID 5)	12.9 GB
				Usable Total: **17.2 GB**	

Firewall Administration

The AltaVista Firewall software was administered using a remote management station configured with AltaVista Tunnel, as described in the following procedures.

Starting a Tunneling Session

To connect to the firewall from the remote system:

1. Insert the diskette containing the crypto key in the floppy drive. (This diskette is created when a remote management channel is setup on the firewall system. See the section on Remote Firewall Administration in Chapter 4.)
2. Run AltaVista Tunnel.
3. From the Tunnels pull-down menu, select Add.
4. Navigate to the floppy drive and double click the `.eta` file. The AltaVista Personal Tunnel dialog box is displayed, populated with the data from the `.eta` file.
5. Click the Connect button.
6. When prompted, enter the password you assigned when you created the remote channel. A log of the handshake is displayed at the bottom of the screen. The client is authenticated through the firewall and a tunneling session is started.

Monitoring Firewall Activity Remotely

AltaVista Tunnel uses the Netscape browser to monitor the activity of the firewall and display the log file of firewall events.

To monitor the firewall from the remote management system:

1. Start the Netscape browser on the remote host.
2. In the Location field, enter the Firewall Virtual IP address you assigned when you created the remote management channel (Table 4-3), followed by the port number, :8314. In the HiTest example, this is 192.168.1.204:8314 .

   When you access this location, the firewall user interface displays on the remote host. You can now control the firewall from the remote host. Although alarms cannot be adjusted remotely, all other operations are allowed.
3. Disconnect the tunnel when you are finished working to protect the security of your network.

Test Process and Results

This section describes the test processes used by the HiTest team and describes the results of the tests.

HyperText Transfer Protocol (HTTP)

Web browsing from the internal (blue) network to the external (red) network was accomplished by configuring a web browser with the firewall server `broots.abc.doc.com` as the proxy. Webstone was operated from within the internal network by specifying `broots.abc.doc.com` as a proxy.

Web browsing from the external (red) network to the internal network was accomplished by specifying the firewall external IP address as the proxy. The web proxy service on the firewall was configured to allow networks with internal IP addresses and the external firewall IP address to pass through the proxy.

File Transfer Protocol (FTP)

The FTP proxy was configured to allow full access to the external network (Gets and Puts). It was configured to allow authenticated access from the external network.

From the blue network to the red the following commands were used:

1. **`C:\>`** `ftp` *`host.domain`*

   For example:

   `ftp broots.abc.doc.com`

   The server responds with a welcome message

2. **user:** *`user@host.domain`*

   For example, for a UNIX machine in the external network:

   `root@foobar.efg.doc.com`

3. **password:**`********`

   ftp>

From the red network to the blue network the following commands were used:

1. **`C:\>`** `ftp` *`nn.nnn.nn.nn`*

   or

   `C:\>` `ftp` *`host.domain`*

   where *`nn.nnn.nn.nn`* is an IP address and *`host.domain`* is a host and domain in the external network.

   For example, ftp 16.123.45.67

   The firewall responds with a welcome message

2. **`user:`** `anonymous`*`@host.domain`*

   For example, `anonymous@veroni.abc.doc.com`

3. **password:**`**********`

4. **ftp**>quote `authenticate` *`username/password`* (NT account)

   The firewall responds with "Logon Success"

   ftp>

Simple Mail Transfer Protocol (SMTP)

From the internal network, Exchange clients sent mail to the Exchange server in the external network. The Exchange server SMTP connector on Veroni was configured to forward mail to internal address of the firewall server.

From the external network, Lotus Notes clients running automated scripts sent mail by way of an SMTP Message Transfer Agent on a Domino SMTP server to the IP address of the firewall server. The firewall forwarded the mail to the internal Exchange Server.

Telnet

From the internal network to the external network, the following commands were used:

1. **C:\>** telnet *host.domain*

   For example, `telnet broots.abc.doc.com`

   The firewall responds with a telnet window and welcome message.

2. **command ?** authenticate *username/password*

   The firewall responds with the message "Logon Success".

   command ?

From the external network to the internal network, the following commands were used:

1. **C:\>** telnet *nn.nnn.nn.nn*

   or

   C:\> telnet *host.domain*

   where *nn.nnn.nn.nn* is an IP address and *host.domain* is a host and domain in the external network.

   For example,

   `telnet 16.123.45.67`

   Firewall responds with a telnet window and welcome message

2. **command ?** authenticate *username/password*

   Firewall responds with "Logon Success"

3. **command ?**

Interoperability Test Results

The HiTest interoperability test results established the data integrity for messages passing through the HiTest firewall. These results do not represent system limits because the monitoring of data integrity does not reflect performance in normal use. These tests are not characterization tests.

The following information describes the test results for the 40 hour Maximum and Minimum configuration tests:

- Approximate web transfers from external (red) network to internal (blue) Webstone client: 660500 web pages.
- Approximate web transfers from internal (blue) network to external (red) network generated and verified with LotusScript: 42000 web pages.
- Approximate mail transfers from external (red) network to internal (blue) network generated with LotusScript: 49000 mail messages.
- Approximate FTP transfers from internal (blue) network to external (red) network generated and verified with LotusScript by way of a DOS window: 200 transfers (average 4.5 kb/sec).
- Telnet operations were demonstrated manually.
- Alarm operations were verified manually.
- Remote administration was successful.

Workload Characterization Test Results

Table 5-3 shows the results of the workload characterization tests performed by HiTest:

Table 5-3: Workload Characterization Test Results

Type of Test	Minimum	Maximum	Average
Files transfered using FTP	115 KB	500 KB	210 KB
Mail messages	512 Bytes	512 Bytes	512 Bytes
Web pages	1 KB	33 KB	16 KB

6
Problems and Solutions

This chapter describes problems encountered during the testing. Where appropriate, a solution for each problem is given which provides a fix or workaround. An impact statement is also provided.

Foundation Hardware

No problems were encountered.

Foundation Software

No problems were encountered.

AppSet Software

The following problems were identified:

SMTP Proxy Validation

Problem **Fake mail is not allowed through the firewall**

Although the NT registry entry is set to allow fake mail (mail from a source that cannot be verified by DNS), fake mail is not allowed through the firewall.

Impact **Low**

This problem should not occur if the instructions for installing AltaVista Firewall 97 in Chapter 4 are followed.

Solution **Upgrade the SMTPXD.EXE daemon**

Download the new SMTPXD.EXE daemon, which is available from the AltaVista support web page at: `http://support.altavista.digital.com`. Procedures are included as a readme file when downloading the patch. For more information, see the section on AltaVista Firewall 97 Installation in Chapter 4.

If you do not download the new SMTPXD.EXE file, DNS entries are required for any system from which you want to receive mail.

NT Domain Authentication

Problem **Underscores not allowed in NT domain authentication**

The firewall user interface does not allow underscores when configuring the system to use NT domain authentication.

Impact **Low**

This problem should not occur if the workaround in Chapter 4 for authenticating a domain name with underscores is followed.

Solution **Enter a name without underscores, then modify it**

When setting up authentication, enter the domain name without underscores. Later change the domain name in the NT registry. For detailed instructions, see the User Authentication Set Up section of Chapter 4.

7
Detailed Hardware Configuration

This chapter describes the minimum and maximum hardware configuration for the AltaVista Firewall Windows NT AlphaServer 800 HiTest Suite by providing the following:

- System Diagram
- HiTest System Slot Configurations
- Input/Output Slot Usage
- Storage Architecture

System Diagram

Figure 7-1 shows a diagram of the maximum configuration of this HiTest Suite. Table 7-1 lists the major cables.

Figure 7-1: System Diagram

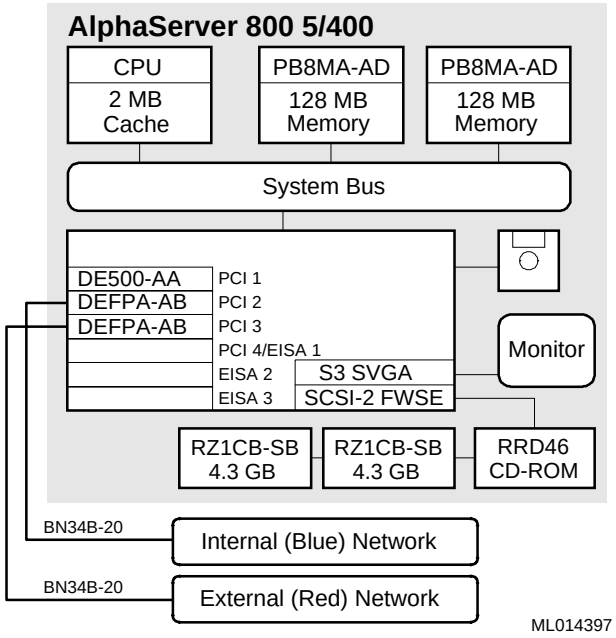


Table 7-1: Configuration Cabling

Part Number	Qty	Description	From	To
BN34B-20	2	20-m SC to SC dual fiber optic cable	DEFPA-AB	External and Internal networks

HiTest System Slot Configuration

Figure 7-2 shows the HiTest System Slot Usage and Table 7-2 describes the minimum and maximum hardware configurations used in this HiTest Template.

Figure 7-2: HiTest System Slot Usage

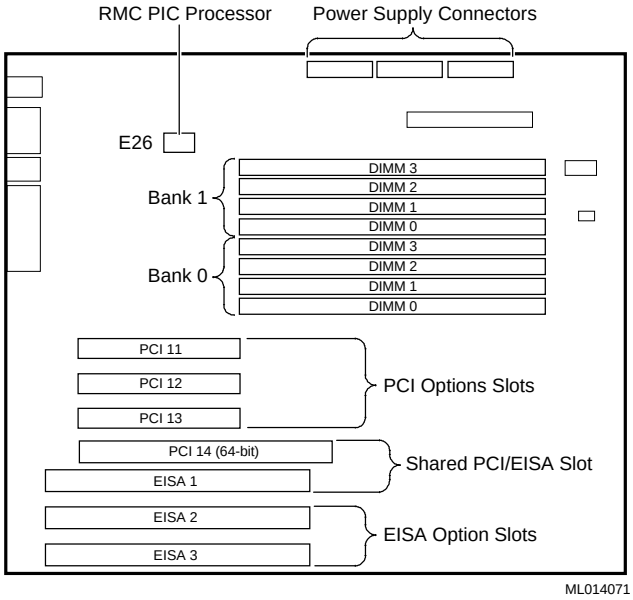


Table 7-2: System Slot Usage (Minimum and Maximum Configurations)

Slot	Minimum Configuration	Maximum Configuration	Description
DIMM3	open	PB8MA-AD (32 MB)	Memory Bank 1 (4 of 4)
DIMM2	open	PB8MA-AD (32 MB)	Memory Bank 1 (3 of 4)
DIMM1	open	PB8MA-AD (32 MB)	Memory Bank 1 (2 of 4)
DIMM0	open	PB8MA-AD (32 MB)	Memory Bank 1 (1 of 4)
DIMM3	PB8MA-AD (32 MB)	PB8MA-AD (32 MB)	Memory Bank 0 (4 of 4)
DIMM2	PB8MA-AD (32 MB)	PB8MA-AD (32 MB)	Memory Bank 0 (3 of 4)
DIMM1	PB8MA-AD (32 MB)	PB8MA-AD (32 MB)	Memory Bank 0 (2 of 4)
DIMM0	PB8MA-AD (32 MB)	PB8MA-AD (32 MB)	Memory Bank 0 (1 of 4)

Input/Output Slot Usage

Table 7-3 and Table 7-4 show the input/output (I/O) slot usage for the minimum and maximum configurations of this HiTest Template.

Table 7-3: I/O Slot Usage (Minimum Configuration)

Slot	Minimum Configuration	Description
PCI-11	DE500-AA	Fast Ethernet Adapter
PCI-12	DE500-AA	Fast Ethernet Adapter
PCI-13	open	–
PCI-14 / EISA-1	open	–
EISA-2	open	–
EISA-3	open	–

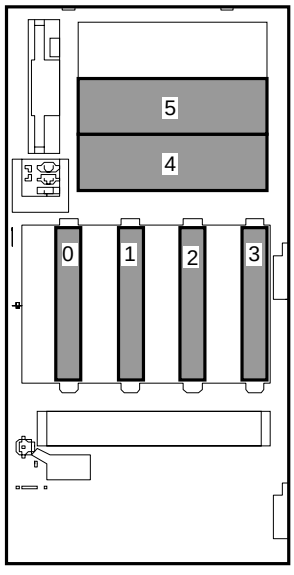
Table 7-4: I/O Slot Usage (Maximum Configuration)

Slot	Maximum Configuration	Description
PCI-11	DE500-AA	Fast Ethernet Adapter
PCI-12	DEFPA-AB	FDDI Adapter
PCI-13	DEFPA-AB	FDDI Adapter
PCI-14 / EISA-1	open	–
EISA-2	open	–
EISA-3	open	–

Storage Architecture

Figure 7-3 shows the storage architecture used in this HiTest Template. Table 7-5 lists the SCSI storage for the minimum and maximum configurations of this HiTest Template.

Figure 7-3: Storage Architecture



IP00-79A

Table 7-5: SCSI Storage (Minimum and Maximum Configurations)

Slot	Option/ Part Number	Description
0	RZ1CB-SB	Windows NT Server, paging
1	RZ1CB-SB	AltaVista Firewall application, AltaVista Tunnel application, data (including web pages), log file, paging file (300-700 MB) and file share
4	DS-RRD46-VA	600 MB 12X SCSI CD-ROM Drive