Software Product Description

PRODUCT NAME: AltaVista Tunnel 98 **SPD 56.13.05**

DESCRIPTION

AltaVista Tunnel allows you to use the public Internet as a secure, cost-effective extension to your private corporate network. This type of networking environment is called a Virtual Private Network (VPN). You securely link remote offices, business partners, and telecommuters with Internet connections, dramatically reducing your network costs.

The following environments are made possible with AltaVista Tunnel:

- Telecommuting - users connect to their private network through a high-speed connection via a local Internet Service Provider (ISP) and the Internet.
- Remote Office - IP traffic from users at a remote site is securely routed over the Internet to the private network at their company's home office.
- Business to Business - extends the Remote Office environment to allow business partners to securely link together.
- Within a Business - only authorized users access sensitive information within their company.

AltaVista Tunnel product offerings include two types of servers: Telecommuter Server and Extranet Server. The Telecommuter Server enables you to securely connect an AltaVista Tunnel Client to a server in a private network via the Internet. The Extranet Server allows you to connect two servers (i.e., two private networks) to support confidential organization-to-organization communications. Thus, there are two typical server configurations:

1. Telecommuter Server-to-Clients - connects telecommuters and mobile workers via the Internet to their corporate network.
2. Extranet Server-to-Extranet Server - primarily connects two or more networks, such as remote office-to-headquarters or business partner-to-business partner, via the Internet. Clients, such as telecommuters, are also allowed to connect to Extranet Servers.

In both server configurations, the end point of the connection must be an AltaVista Tunnel Server for tunnel authorization, authentication, and management.

The terms AltaVista Tunnel, tunnel, or tunneling may be used when referring to both AltaVista Tunnel Server and AltaVista Tunnel Client. The term Server will be used when referring to both AltaVista Tunnel Telecommuter Server and AltaVista Tunnel Extranet Server.

WHAT IS TUNNELING?

Tunneling allows information to be securely passed between one computer and another over a public network, such as the Internet, as if the computers were on the same physical network. The process of sending information through tunnels is simple and straightforward. After authenticating the tunnel client and the tunnel server, information is encrypted by its sender, encapsulated into TCP/IP data packets, and sent across the Internet as unreadable and unrecognizable data. Once the packets reach their final destination, they are reconstituted, and decrypted into a readable form.

A system running the Client or Server software may act as a tunnel client, while only a system running the Server may be a tunnel server (with management capabilities).

AUTHENTICATION, ENCRYPTION AND DATA INTEGRITY

AltaVista Tunnel employs RSA Public Key Cryptosystem (1024-bit in US version and 512-bit in International versions) for user authentication and session key exchange, and RSA RC4 Symmetric Stream Cipher for bulk data encryption. Cryptographic identity and keys are tied to the user, leaving the IP address free to be dynamically assigned. Once the authenticated tunnel session is created, the tunnel server and tunnel client automatically switches from public key encryption to RC4-based secret key encryption to perform bulk data encryption and transmission. At 30-minute intervals, the tunnel client and server exchange new session keys. During data packet transmission, each packet is integrity protected and authenticated by MD5.

In conformance with federal export regulations, the US version of the AltaVista Tunnel product employs a 128-bit RC4 key, while the International version supportsa 56-bit RC4 key (40-bit RCA key product offerings are also available, if required).

AltaVista Tunnel supports the optional use of Security Dynamics' SecurID authentication tokens (SecurID Card, KeyFob, and PinPad) to authenticate the identity of users. The tunnel administrator designates a tunnel as requiring SecurID authentication. When a tunnel client connects, the tunnel server instructs the tunnel client to prompt the user for SecurID credentials. This information is sent to the tunnel server for processing (the tunnel server is an ACE/Client acting as a proxy to the tunnel clients). The tunnel client is then either authorized or unauthorized to connect. The tunnel client also supports NEWPIN and NEXTCODE modes to complete the SecurID implementation.

When creating a multinational tunnel, automatic arbitration reconciles any encryption discrepancies transparently. This enables both the tunnel client and server to operate in the highest common encryption key mode supported.

This product is classified as "ITAR (International Traffic in Arms Regulations) Controlled." The usage and intent of this sensitive product shall therefore comply with any related export and import laws.

DATA COMPRESSION

Data compression reduces redundancy in data representation in order to decrease storage and communication costs, and increase performance. AltaVista Tunnel supports the use of LZO compression as its optional compression technique. The inbound tunnel server always has compression enabled. The outbound tunnel system dictates whether compression is used. If both tunnel systems have compression enabled, compression is used; otherwise, tunnel traffic is not compressed.

NETWORK INTEGRATION

AltaVista Tunnel takes advantage of the private network's environment capabilities. AltaVista Tunnel adds the private network's DNS server automatically when users are running the tunnel client. The tunnel administrator can select the DNS server for all tunnel client connections. For Windows 95 and Windows 98 clients, the private network's WINS server can be specified for WINS name resolution.

TUNNEL MANAGEMENT

The AltaVista Tunnel management key features and graphical user interface simplify tunnel management, eliminating the need for a dedicated administrator. In a client-to-server tunnel environment, the server performs all tunnel management. In a server-to-server or organization-to-organization tunnel environment, either server can perform these management tasks:

- Connection authorization
- Public key generation and management (*)
- Tunnel parameter management
- Dynamic assignment to tunnel clients
- Tunnel-related routing change monitoring
- Tunnel usage statistical report generation
- Tunnel deletion

Note: The Server employs a key generation tool for creating the public-private key pairs for all tunnels. The tunnel administrator generates all public-private key pairs and maintains tunnel server key rings.

FIREWALL INDEPENDENCE

Most Internet-connected corporations and organizations employ firewalls to protect the information on their private networks from Internet invaders. Because AltaVista Tunnel uses encryption and authentication to protect that information as it is transmitted across the Internet, it is a natural complement to any firewall. AltaVista Tunnel Server can run on a system with AltaVista Firewall or it can run on a separate system behind a firewall that protects it from the Internet.

APPLICATION INDEPENDENCE

AltaVista Tunnel seamlessly integrates into an existing corporate network environment. Since it is a flexible IP-based solution operating at the network layer, there is no need to modify any existing applications.

Primary Components of the AltaVista Tunnel Server are:

- Tunnel pseudo device driver
- Tunnel service (Windows NT, daemon - DIGITAL UNIX)
- Windows-based server user interface (Windows NT)
- Motif-based server user interface (DIGITAL UNIX)
- Native installation and configuration procedure

Primary Components of the AltaVista Tunnel Client are:

- Pseudo-adapter device driver (Windows 95, Windows 98, and Windows NT)

- Open Transport STREAMS modules (Mac OS)
- Windows-based client user interface
- Online Help
- Native installation procedure

The AltaVista Tunnel Client for Microsoft Windows systems is based on Microsoft's TCP/IP stack, an integral part of the Windows-based operating systems. The AltaVista Tunnel Client for Mac OS systems is based on the Open Transport Networking stack.

HARDWARE REQUIREMENTS

Processors Supported:

- Server: Intel Pentium 90 or higher, DIGITAL Alpha processor
- Client: Intel 80486 or higher, DIGITAL Alpha processor, PowerPC processor

The processor must include a monitor and be capable of supporting a network interface card or adapter.

Other Hardware Required:

In general, AltaVista Tunnel provides enhanced security to TCP/IP network transmissions over the Internet. Thus, all the hardware (e.g., modems) necessary to implement a remote TCP/IP networking environment should already be in place. No additional hardware is required.

To install the AltaVista Tunnel software, the system must either support a CD-ROM reader or be able to connect to a network file share.

Minimum Disk Space Requirements:

- Server: 15 MB for Windows NT; 25 MB for DIGITAL UNIX
- Client: 5 MB for Windows 95, Windows 98 and Windows NT; 3 MB for Mac OS

Minimum Memory Requirements:

- Server: 48 MB for Windows NT (Intel); 64 MB for Windows NT (Alpha); 64 MB for DIGITAL UNIX
- Client: 16 MB for Windows 95 and Windows 98; 32 MB for Windows NT; 16 MB for Mac OS

SOFTWARE REQUIREMENTS

Operating Systems Supported:

- Server: Windows NT 4.0 (Service Pack 3 or higher); DIGITAL UNIX V4.0A or higher
- Client: Windows 95; Windows 98 (NOTE: Service Pack 2 (via "AltaVista Tunnel 98 for Windows 98 Service Pack" or an updated Client kit) is required); Windows NT V4.0; Mac OS supporting Open Transport Networking V1.1.1, V1.1.2, V1.2 or V1.3

AltaVista Tunnel 98 Client for Mac OS is compatible only with AltaVista Tunnel 98 Server. AltaVista Tunnel 98 Clients for Microsoft Windows systems are also compatible with AltaVista Tunnel 97 Workgroup Edition. It is strongly recommended to upgrade all servers to AltaVista Tunnel 98 Server.

Other Software Requirements:

All the software (e.g., dial-up networking) necessary to implement a TCP/IP networking environment must already be in place. For Windows 95 clients, the Microsoft Dial-Up Networking V1.2 patch is required to use dial-up networking with AltaVista Tunnel.

GROWTH CONSIDERATIONS

The AltaVista Tunnel Server for the Windows NT platform supports up to 200 concurrent tunnel connections. The AltaVista Tunnel Server for the DIGITAL UNIX platform supports up to 2000 concurrent tunnel connections.

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

DISTRIBUTION MEDIA

All AltaVista Tunnel software is available on CD-ROM. Client 3.5" floppy kits can be created from the AltaVista Tunnel 98 Client CD-ROM.

AltaVista Tunnel Server is not available as part of the DIGITAL UNIX Consolidated Software Distribution on CD-ROM.

For available patches to known problems, visit the Downloads area of the AltaVista oftware site: http://altavista.software.digital.com

ORDERING INFORMATION

The AltaVista Tunnel Server is available on Windows NT (Intel and Alpha) and DIGITAL UNIX. Server options include the following:

- Telecommuter Server (includes 2 client licenses)
- Extranet Server (includes 2 client licenses)

The AltaVista Tunnel Client is available on Windows 95, Windows 98, Windows NT (Intel and Alpha), and Mac OS. The AltaVista Tunnel 98 Client for Mac OS client is packaged separately.

AltaVista Tunnel includes U.S./Canada (128-bit) and International (56-bit and 40-bit) part numbers based on Unique Product Identifiers (UPIs):

Encryption Level:	Server UPI	Client UPI
U.S./Canada (128-bit)	4W0	4W2
International (56-bit)	4W1	4W3
International (40-bit)	5VQ	624

For further ordering information, contact your local DIGITAL office or authorized AltaVista Business Partner.

SOFTWARE LICENSING

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

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

SOFTWARE WARRANTY

A Limited Warranty for this software product is provided by DIGITAL with the purchase of this software package.

AltaVista Tunnel 98 is designated "Year 2000 Ready". For warranty information, visit the following site: http://www.digital.com/year2000

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.