Description

With on-site access, the Internet is a flexible, remote extension to your private network, without high costs or security worries. On-site computing provides simple, direct access to information and people no matter where you or they happen to be. It is simple because it uses standard web browsers to bring the Internet to your company’s intranet. On-site computing means speed: you can do work from any location, and fast communication means having the competitive edge.

Wherever you are, you are connected to your company’s private network. You can easily and securely connect to firewall-protected branch offices, divisions and partners. You can use the Internet for real business by creating a highly-secure connection with the information, people and resources that reside behind your corporate firewalls.

Wherever you’re located, and even if you frequently change locations, you’ll always have on-site access. Unlike a leased line that continuously links two sites, AltaVista tunnel is dynamic: it can be instantly brought up or taken down from wherever you are, connecting to any of your preferred business sites.

Using the global Internet as the backbone infrastructure, AltaVista tunnel creates virtual private networks (VPN), extending the reach of your intranet without jeopardizing the security of valuable information assets. It is easy — if you can point-and-click, you can create a secure tunnel — anywhere, any time — and securely, cost-effectively connect with partners, suppliers, mobile workers, telecommuters and customers.
AltaVista tunnel is available in group and client versions. The group version creates a secure connection between remote networks, while the client version allows a single remote user to link into a group. The AltaVista tunnel products offer the secure on-site access for which Internet users have long been waiting.

The AltaVista tunnel uses the public Internet as a secure, cost-effective extension or alternative to your private network. The client or personal version enables you to securely connect a personal computer to a server in a private network via the Internet. The group (server) version lets you connect two servers or two private networks to support confidential organization-to-organization communications. Thus, there are two possible configurations: 1) group to group and 2) a group to client. In both, one end point must be a server for tunnel authorization, authentication, and management.

Tunneling allows information to be securely passed between one computer and another over a public network as if the two were connected by a single physical wire. 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. Note that a system running group or client software may be a client, while only a system running the group software may be a server (tunnel management station).

The AltaVista tunnel employs RSA Public Key Cryptosystem (512 bit) for 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 switch 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 pass new session keys back and forth to decode transmitted data. During data packet transmission, each packet is integrity protected and authenticated by MD5.

In conformance with federal export regulations, the U.S. version of the AltaVista tunnel employs a 128-bit RC4 key, while the international version supports a 40-bit RC4 key. When creating a multinational tunnel, automatic arbitration reconciles this key discrepancy transparently, enabling both the tunnel client and server to operate in common key mode.

Most Internet-connected companies and organizations employ firewalls to protect the information on their private networks from Internet invaders. Because the tunnel uses encryption and authentication to protect that information as it is transmitted across the Internet, it is a natural complement to any firewall. However, a firewall is not a prerequisite for the tunnel which delivers a highly flexible firewall-independent solution. The group tunnel software can run on a system with the AltaVista firewall or it can run on a separate system behind a firewall that protects it from the Internet.

The AltaVista group tunnel management features and interface simplify tunnel management and eliminate the need for a dedicated administrator. In a personal-to-group tunnel environment, tunnel management is performed by the group tunnel server. In a group-to-group or organization-to-organization environment, either one of the group tunnel servers can perform these management tasks:

- Connection authorization.
- Tunnel parameter management.
- DHCP-style address assignment to tunnel clients.
Public key generation and management - The group tunnel employs a key generation tool for creating the public-private key pairs for all tunnels. The tool is not supplied with the personal tunnel client and will be available only for platforms on which the tunnel server runs. The tunnel administrator generates all public-private key pairs and maintains server tunnel key rings.

- Tunnel-related routing change monitoring.
- Tunnel deletion.

Specifications

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows NT 4.0</td>
</tr>
<tr>
<td>Server or client workstation</td>
<td>Pentium 90 or higher</td>
</tr>
<tr>
<td>CD-ROM reader</td>
<td>Required for installation</td>
</tr>
<tr>
<td>Disk space</td>
<td>10 Mb for Windows NT</td>
</tr>
<tr>
<td>Memory</td>
<td>32 Mb</td>
</tr>
<tr>
<td>Concurrent tunnels supported by each license</td>
<td>Group: 10</td>
</tr>
<tr>
<td></td>
<td>Client: 1</td>
</tr>
</tbody>
</table>

Note:
1. In general, the AltaVista tunnel enhances TCP/IP network transmissions with additional security and integrity. Thus, all the hardware and software (e.g., ethernet adapters and dialup networking) necessary to implement a TCP/IP networking environment should already be in place. The tunnel requires no additional hardware or software besides the tunnel product itself.

Nomenclature

<table>
<thead>
<tr>
<th>Description</th>
<th>Nomenclature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group license</td>
<td>S-PB-TNL-QB-4W0AC-SB</td>
</tr>
<tr>
<td>Client license</td>
<td>S-PB-TNL-QB-4W2AB-SA</td>
</tr>
<tr>
<td>only</td>
<td>S-PB-TNL-QB-4W3-AB-SA</td>
</tr>
</tbody>
</table>
Our worldwide staff of professionals is ready to meet your needs for process automation. For the location nearest you, please contact the appropriate regional office.

AMERICAS
29801 Euclid Avenue
Wickliffe, Ohio USA 44092
Telephone 1-216-585-8500
Telefax 1-216-585-8756

ASIA/PACIFIC
152 Beach Road
Gateway East #20-04
Singapore 189721
Telephone 65-391-0800
Telefax 65-292-9011

EUROPE, AFRICA, MIDDLE EAST
Via Puccini 2
16154 Genoa, Italy
Telephone 39-10-6582-943
Telefax 39-10-6582-941

GERMANY
Graefstrasse 97
D-60487 Frankfurt Main
Germany
Telephone 49-69-799-0
Telefax 49-69-799-2406