Digital’s Internet Tunnel Products

White paper: Virtual private networking over the internet — today
# Table of Contents

3  What is tunneling?

3  Benefits of using the Internet for private networking

3  Encryption, firewalling, and Digital’s tunnel architecture

4  How it works

4  Product descriptions:
   - Digital Internet Group Tunnel
   - Digital Internet Personal Tunnel

5  Frequently asked questions

7  Glossary of acronyms
Have you, like a growing number of corporations, considered reducing your telecom costs by using the Internet to connect your remote LANs together — yet worried about whether your sensitive information can be transmitted over the public Internet, secure from both external and internal unauthorized users?

As a remote worker using a PC on the road or at home, have you been frustrated because your local Internet service provider can’t get you past the firewall at your employer’s network?

Do you want to know who is accessing your network, and ensure that only authorized parties have access?

If your answer is yes, this White Paper from Digital Equipment Corporation describes a unique solution meeting these needs — Digital’s Internet Tunnel products, bringing you the speed, cost-effectiveness and security of virtual private networking over the Internet.

1. What is tunneling?

Tunneling has been used in computer networking for years. It is a method of transporting data from one point to another, encapsulating the data in wrapper packets. For example, one can tunnel Novell® IPX traffic in TCP/IP. The source and destination of the encapsulated traffic do not know that the data has traveled through a tunnel. All applications work normally and without modification.

Digital’s Internet Tunnel is an encrypted tunneling product. Encrypted tunnels are no different in concept from standard tunnels. However, instead of a protocol like IPX being encapsulated, regular IP packets are encrypted and then encapsulated inside a TCP/IP packet. The source and destination IP applications work as normal, but the data on the network between the two tunnel servers appears scrambled. Encrypted tunnels are discussed in more detail in section 3.

2. Benefits of using the Internet for private networking

With the growth, stability, and declining costs of the Internet, there is increasing interest in replacing expensive private network bandwidth with low-cost, public bandwidth — using connections to the Internet backbone.

Such a strategy results in cost efficiencies, including:

- Less communications equipment
- Consolidated data circuits
- No more long-haul circuits

Each facility of an enterprise with a LAN environment connects the LAN with a high-speed line to a local Internet Service Provider (ISP). The Internet is then the high-speed backbone of the enterprise, rather than a mesh of private data circuits. The result is a form of virtual private networking using the Internet rather than a private frame relay or ATM network.

The major concerns in building virtual private networks (VPNs) are security, reliability, and performance. Reliability and performance are quite good today, assuming the ISP provides high-speed connections to the Internet and a full-time support staff. Security is provided using encrypted tunnel technology. This leaves security issues as the main focus of concern.

3. Encryption, firewalling, and Digital’s tunnel architecture

As a key to security, encrypted tunnels are starting to be discussed by major networking vendors. By the end of 1995, there will be several products available. There are no standards yet, and each method is a bit different. As a result, solutions from different vendors are not yet interoperable.

Digital’s tunnel architecture provides a high degree of flexibility and security by being firewall-independent. Digital is active in standardization efforts to hasten interoperability among tunnel vendors. Digital’s products are here today, and are based on many years of research and experience in network security.

Enterprise LANs that are connected to the Internet typically have some form of firewall technology to create a trusted administrative domain separate from the Internet. A firewall regulates and logs interaction between trusted and untrusted networks. Local policy decides what is allowed. Many sites will allow trusted users to initiate connections to the Internet, but allow very restricted access from the Internet to their trusted network. When building a VPN using tunnels, policy is set with the firewall to allow the encrypted and authenticated data from Internet Tunnel clients into the trusted network. A combination of packet filtering and forwarding relays is used.
Tunneled data remains encrypted past the firewall, and inside the trusted network, until it arrives at a Digital Internet Group Tunnel server. The Group Tunnel server can be placed on the same LAN as the firewall, or anywhere on the private network. This gives the flexibility to maintain security within a semi-trusted domain. The tunnel server may be on a personnel, financial, or research LAN, making sure that sensitive data does not pass in clear text across other parts of the enterprise.

Other vendors plan to offer host-to-host or LAN-to-LAN VPNs. Digital’s Internet Tunnel strategy provides an additional configuration supporting direct tunnels from PCs. The Internet Personal Tunnel makes use of client software running on a Windows® 95-based PC linked over the Internet to an Internet Group Tunnel server. The Group Tunnel server can handle many PC tunnel clients, and many LAN-based network tunnels at the same time. The network manager controls access to incoming tunnel connections by authorizing individual users or remote LANs.

Digital’s Internet Personal Tunnel technology is unique in the market today. It allows the PCs of home-based or mobile users to connect to any Internet Service Provider and construct a secure tunnel into their corporate network. The tunnel enables the user to be a virtual member of the trusted network. A personal password or Personal Identification Number (PIN) number is used to guard against misuse of the PC, and an encryption key pair is used to authenticate the specific PC with a specific trusted tunnel server. Authorization is based on a user name, not an IP address, so users can roam the network and not be tied to a specific address. Once the tunnel has been constructed to the trusted network, the PC can communicate anywhere within the network, or be restricted by policy to specific hosts or LANs. No additional software is required inside the trusted network, since normal routing is used once the packets are out of the tunnel and decrypted.

Use of the Internet Personal Tunnel can lower costs by reducing the volume of equipment needed to support dial-in networking for employees. Fewer dial-in lines and modems are required, and the task of network management is reduced. Security is also enhanced by strong authentication of dial-in users. The same high-speed connection to the Internet that provides the site with enterprise and worldwide access is also used for dial-up users. Dial-up users connect to their local ISP, reducing long distance charges. No software is required on the ISP’s network, and all data through the ISP’s network and the Internet is encrypted.

Digital’s Internet Tunnel products is limited to a 40-bit RC4 key. The Digital Internet Tunnel negotiates the key size during tunnel setup, so U.S. and Canadian network sites can communicate domestically or internationally, all with the same product.

4. How it works
When a tunnel client (group or personal) wants to initiate a connection with an Internet Group Tunnel server, a connection request is sent over the network. The request may actually be addressed to a firewall, which relays the connection to the proper Internet Group Tunnel server.

The connection request message contains an identification message that is encrypted by the client with the server’s public key, and then decrypted by the server with its own private key.

The server’s database contains a list of clients that are authorized to build tunnels. If the request is to be granted, the tunnel server sends a response encrypted using the client’s public key, which is then decrypted by the client using its private key. After this authentication sequence, the two parties exchange portions of a session key, which are combined to form a secret session key. Session keys are periodically changed to enhance security.

The tunnel client is issued an IP address that is valid for the network of the Group Tunnel server. The tunnel client in effect has two addresses. One is appropriate for the network the client is directly connected to, and the other is appropriate for the network that has been tunneled into. The routing tables of the client are set up so that all communication intended for hosts on the network tunneled into are sent through the tunnel. All communication intended for hosts other than on the tunneled network are sent normally through the directly connected network.

5. Product descriptions:

Digital Internet Group Tunnel
This is a layered software product that is installed on the Digital UNIX® operating system running on a Digital Alpha
A network (SLIP, PPP, Ethernet, or FDDI) connection is required. The tunnel software can share the system with other software, but the system should be managed as a highly trusted system since it generates authentication keys and authorizes remote tunnel clients.

The Internet Group Tunnel software manages the construction and operation of tunnels from other Internet Group Tunnel servers or Internet Personal Tunnel servers. Performance is based on system configuration and end-to-end network throughput. A tunnel server can support up to 512 tunnel connections.

An Internet Group Tunnel can act as a client only, a server only, or a client and server at the same time. It can be the server for many Personal Tunnel clients, and other Group Tunnels acting as clients, while itself acting as a tunnel client to construct a tunnel to another Group Tunnel server. Tunnels are always initiated by a client and authorized by a server.

Authentication key generation and management software is included with the Internet Tunnel product. The keys are used to identify and verify tunnel end points that wish to construct an active tunnel. Authentication is based on users, not host address. This permits users to roam.

Management software included with the Internet Group Tunnel is used to authorize users, generate keys, view active tunnels, and disconnect tunnels.

Packet filter software in Digital UNIX is used to enforce access policy for PCs and networks coming in through an encrypted tunnel. This software is flexible enough to create a different policy for each tunnel.

**Digital Internet Personal Tunnel**
This software is installed on a PC running Microsoft’s Windows 95 software. It enables the user of the PC to build a tunnel to a Digital Internet Group Tunnel.

The PC must have the Windows 95 TCP/IP software active, be connected to a network with connectivity to the desired remote network, and be using a valid IP address for the local subnet.

Authentication keys are provided to the Internet Personal Tunnel software from the key-generation software that is supplied with the Internet Group Tunnel software. A different key will be used for each unique Group Tunnel that is to be connected to and each user that may use the PC to construct tunnels.

The Internet Personal Tunnel software includes a WIN32® Windows-based application to allow the user to request, operate, and manage an encrypted tunnel. The user specifies a remote tunnel server and a user ID. A PIN is required by the Personal Tunnel software before the tunnel is constructed. This helps prevent unauthorized use of the software. Authentication keys are stored on the PC in an encrypted form, using the PIN as the key. A log window is provided to show the progress of tunnel construction and status of the active tunnel.

**6. Frequently asked questions**

**Q:** “If two Internet Group Tunnels are purchased, what other components would actually be needed to replace a private transatlantic WAN?”

**A:** To replace a private transatlantic WAN, a connection to the Internet from each side of the Atlantic would be made. This would normally require a router and a data circuit to an Internet Service Provider. It is wise to discuss the network topology with potential ISPs, gaining an understanding of the potential throughput between sites and the number of hops and carriers that your data will transit. Using the Internet can be faster or slower than a private network, depending on these factors. It is also wise to understand the government restrictions pertaining to the use of encryption products.

**Q:** “What’s the difference between Digital’s tunneling technology and the technology offered by router and firewall vendors?”

**A:** Digital’s solution offers a more flexible way to build a VPN than other vendors. The support of the Internet Personal Tunnel means that connections from home or on the road into a corporate network are now possible.

Routers offering encryption often only provide it for a single private data circuit, and do not support end-to-end or trans-Internet privacy.

Firewall vendors that support tunneling require the use of their tunnels at both ends, since there are no interoperability standards yet.
Digital’s tunnel products work with many vendors’ firewalls. The server can be placed on the appropriate LAN, so data across semi-secure parts of a corporate network can remain private. The tunnel servers run as a layered product on a Digital UNIX system, meaning that a system does not need to be dedicated to provide the tunnel functions. Assuming pending approvals from the U.S. government, Digital’s tunnel software is among the first approved for international use.

Q: “What encryption technology is being used in Digital’s encrypted tunnel products?”

A: Each tunnel pair uses a unique public/private key pair to authenticate itself to each other. This key uses RSA key-generation tools. Once the tunnel is established, a secret RC4 key is exchanged via the private/public scheme. Data is encrypted using the secret key. Versions for the U.S. and Canada use a 128-bit RC4 key. International versions use a 40-bit RC4 key. When a domestic version connects with an international version, key size is negotiated down to 40 bits.

Q: “Will I have to get special applications to make use of the tunnel?”

A: No. The PC tunnel uses a pseudo-network layer under the transport layer of the IP stack. Any TCP or UDP packet with a destination inside the trusted network will be encrypted, encapsulated, sent to the other end of the tunnel, and delivered unmodified to the destination.

Q: “Will Digital’s tunnel products work with any firewall?”

A: Most firewalls will be able to be set up to allow encrypted tunnel traffic into a trusted network and onto the tunnel server. However, tunnels provide powerful access rights to trusted networks, so some care in selecting the method of bypass is warranted.

One good approach is to set up a generic relay on a firewall. This relays traffic addressed to a unique port on the firewall onto the appropriate port of the Digital Internet Group Tunnel. This method hides the actual address of the Group Tunnel server, and logs all attempts at connection at both the firewall and tunnel. The Digital Internet Tunnel products are tested with the Digital Firewall for UNIX and the BorderWare™ firewall products. Technical tips will be developed for interaction with other firewalls as the information becomes available.

Q: “When using an Internet Personal Tunnel connection from one network to a trusted network, is any routing information exchanged between the two networks?”

A: No. The PC tunnel will have two IP addresses. One will be based on the network that the PC is directly connected to and the other will be a virtual address assigned by the tunnel server. There is no routing enabled in the PC to provide a back door for others on the PC’s connected LAN into the virtual trusted LAN.

Q: “Isn’t all this security stuff replaced by IPV6?”

A: There are a lot of new security enhancements in the upcoming IPV6 protocol, referred to as IPsec. However, it will be at least several years before networks have migrated all their systems to use IPV6. Digital’s tunnel products are an excellent way to use virtual private networking over the Internet today, and during the migration to IPV6. Digital has prototypes of IPV6 protocol stacks running today, and will provide customers with IPV6 products.

Q: “Can I restrict the access of LANs and PCs coming in to my trusted network via tunnels?”

A: Yes. Digital’s tunnel server has a packet filter feature to enforce access policy on tunneled systems. The systems accessing the trusted network via a tunnel can be restricted to access of a single system, a specific subnet or group of subnets, or wide open access.

Q: “If my Internet Personal Tunnel has a tunnel set up, can I access other systems on the Internet? If so, will I pass those packets through my trusted network first?”

A: A PC using the Internet Personal Tunnel software can access policy-permitted systems inside the trusted network as well as systems on the rest of the Internet. Packets not addressed to systems inside the trusted network will not be sent over the tunnel and through the trusted network, but will use normal routing through the ISP to get to the destination.

Q: “Will the tunnel client still work if it has to cross a local firewall before entering the Internet?”

A: Yes, the tunnel client will work, but the policy of the local network may have to be modified to allow tunnel traffic to exit the local network. Firewalls based on packet filtering or circuit filtering technology need only enable the rule to let the traffic pass. If the firewall uses non-transparent application proxy technology, the tunnel client must address the local firewall first, then the remote firewall. Digital’s Internet Tunnel products are designed to address this with a setup parameter that specifies the outgoing firewall’s address.
Q: “Can Digital’s Internet Tunnel products be used to communicate from the U.S. to other countries?”

A: Yes. Encrypted tunnels can be established internationally. Many countries allow the 40-bit RC4 key to be used within their borders, and the U.S. government allows the use of the 40-bit RC4 key from the U.S. to other countries. Some countries prohibit or regulate use of encryption technology within their borders. Some country requirements may be met by a product option to disable the encryption and only use the authentication feature. A list of countries where use of Digital Internet Tunnel products contravenes current law will be available.

Q: “Can a tunnel server act as a router between multiple tunnels?”

A: Yes. The typical case would be a facility that is part of a virtual private network using the Internet Group Tunnel and also wants to support Personal Tunnel users. The same Internet Group Tunnel supports other Internet Group Tunnels and Internet Personal Tunnels at the same time.

Q: “Is there logging of tunnel use?”

A: Yes. The tunnel generates a log for each tunnel that is constructed. The logs are sent to the SYSTLOG for analysis. A system utility on the tunnel server shows the status of live tunnels, and offers commands to disconnect tunnels and perform other management tasks.

Q: “What’s the difference between using tunnel technology and using Netscape’s SSL protocol?”

A: The encryption technology from RSA that is used for SSL and tunnels is similar, but the encryption is done at a different level of the IP stack. SSL encrypts information for applications, while tunnels establish a link for all connections between two networks. Applications that wish to encrypt a specific session, such as Web browsers, Telnet, or FTP must be modified to enable the request for an encrypted link. When using Digital Internet Tunnels, the applications are not modified, and all traffic between tunneled networks is encrypted.

Q: “How is the public key managed? Does it use the SKIP protocol from Sun? Does the product require working with any existing certification authority (CA)?”

A: Key-generation software is included with the tunnel server kit. The keys are based on licensed RSA technology. The key pairs are delivered to remote tunnel clients by floppy, and keys are stored in encrypted form on the tunnel clients and servers. Because the SKIP protocol from Sun is more complex to manage and is not a standard outside the Sun* environment, it is not used in this product. The certificate authority for the keys generated is RSA. However the keys are managed with a PGP-like style of key management, and do not tie into a global hierarchy.

Q: “Can this tunnel technology be used to replace a private wide-area DECnet network or Novell IPX network?”

A: The tunnel only supports the encryption and passing of IP traffic. If the private network traffic has already been converted to IP traffic, then it can be tunneled.

Q: “How can I test-drive Digital’s Internet Tunnel products?”

A: There are two ways to get an evaluation copy of the tunnel products. An evaluation kit of the product may be ordered now for a minimal cost.

A software distribution and evaluation network is expected to be on-line shortly. When operational, you can freely down-line load evaluation kits of the tunnel software. Locate the software distribution site via Digital’s home page (http://www.digital.com/info/internet), by searching for the keyword “tunnel.”

If you don’t have an available Digital UNIX system to set up the tunnel server, you still evaluate the Internet Personal Tunnel software. After down-line loading the tunnel client on a Windows 95 PC, you can create a tunnel to Digital’s evaluation network.

A demo key is built into the evaluation version. It does not have the cryptographic session strength of the purchased product, but has been approved for international distribution by the U.S. government.

Glossary of acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>Asynchronous transfer mode</td>
</tr>
<tr>
<td>FDDI</td>
<td>Fiber distributed data interface</td>
</tr>
<tr>
<td>IP</td>
<td>Internet protocol</td>
</tr>
<tr>
<td>IPX</td>
<td>Internetwork packet exchange</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet service provider</td>
</tr>
<tr>
<td>LAN</td>
<td>Local area network</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-point protocol</td>
</tr>
<tr>
<td>RSA</td>
<td>RSA Data Security, Inc.</td>
</tr>
<tr>
<td>SKIP</td>
<td>Simple key management for internet protocols from Sun</td>
</tr>
<tr>
<td>SLIP</td>
<td>Serial line internet protocol</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure socket layer from Netscape</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission control protocol</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission control protocol/internet protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User datagram protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual private network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide area network</td>
</tr>
</tbody>
</table>