PILOT
NETWORK SERVICES, INC.

Pilot Secure Road Warrior:
Secure Mobile Telecommuting for Corporations

Summary

Pilot Secure Road Warrior is the first service enabling telecommuters to easily and cost effectively connect their laptops to internal corporate networks with high security via any dialup or direct Internet connection in the world. The service offers unprecedented security and scalability.

The growing need for mobile telecommuting

Estimates of worldwide telecommuter usage by the year 2000 run upwards of 50 million users (Gartner Group 1997). Half of these users will be "mobile," connecting from locations such as hotel rooms, branch offices, etc. Increased use of e-mail and web-based information systems across all organizations make being connected critical. Increasingly, employees in remote locations, day-extenders working from home, and traveling executives alike all depend on reliable access to internal network resources securely and cost-effectively.

Yet traditional "remote access" tools can be difficult to support, expensive, and risky. Internal modems and remote access equipment must be correctly configured, monitored, and installed for peak usage levels. Remote users must make long-distance calls, sometimes from overseas, and pay expensive long distance rates in order to connect.

By telecommuting over the Internet, rather than via a direct link, estimated savings of 70% on long distance costs and 50% on modem/remote access support costs can be anticipated (Forrester 1996). Modem banks, and especially grass-roots individual modems, can open large security holes in corporate networks if not tightly managed. The increasing capabilities of desktop operating systems such as Windows NT means that if even one workstation on a network is compromised it can often be used to launch an attack on the entire network. Figure 1 shows the estimated cost savings of leveraging a public network for remote access.

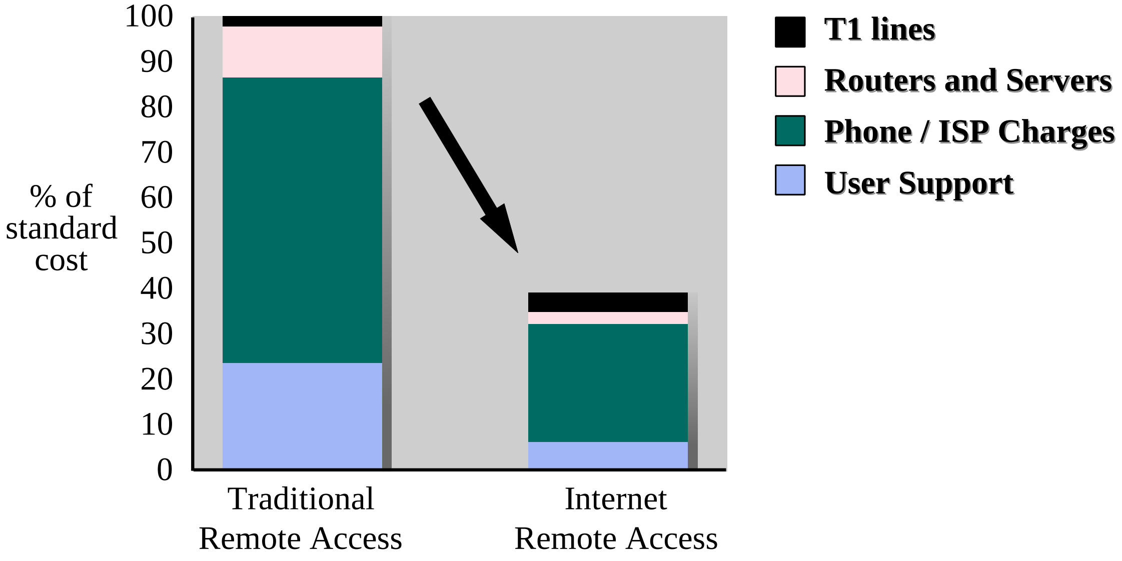

Figure 1: Cost Savings of Remote Access over the Internet (Forrester Research 1996)

<u>Pilot Secure Road Warrior</u>

Instead of dialing an in-house modem directly, Secure Road Warrior enables traveling employees to connect cost-effectively to their corporate network through the Internet and via a Pilot Security Center. Pilot provides a secure dedicated link to the corporate network that establishes a powerful defense against potentially disastrous “back door” security problems. To prevent eavesdropping, traffic is encrypted with a strong 128-bit key. And to keep intruders out, each connection is fully authenticated at Pilot to a specific user and workstation before the traffic reaches the internal corporate network.

Connecting to the Secure Road Warrior service from any location in the world is straightforward, secure and cost-effective. The user dials the most convenient local access provider. Strong, IPSec-compliant encryption software that resides on the laptop computer creates a seamless “encrypted tunnel” from the laptop through the Internet to the Pilot Security Center.

The traffic is monitored, authenticated and decrypted in the Security Center’s “virtual safe room” configured with the Pilot Heuristic Defense Infrastructure™ technology. This multi-layered, constantly upgraded system prevents potential intruders from using the connection as a point of entry into the corporate network. Authorized traffic continues via a secure dedicated connection to the corporate network.

Unlike other telecommuting approaches, the Pilot Secure Road Warrior provides encryption of telecommuters’ data to and from the corporate network *and* protects the network dynamically against intruders. In the ongoing high-stakes battle between electronic intruders and network defenders, increasingly complex hacking can only be countered by continually evolving solutions. And because Pilot’s security infrastructure resides at its Security Centers rather than on a corporate onsite server, its protection is more effective than conventional static firewall software options.

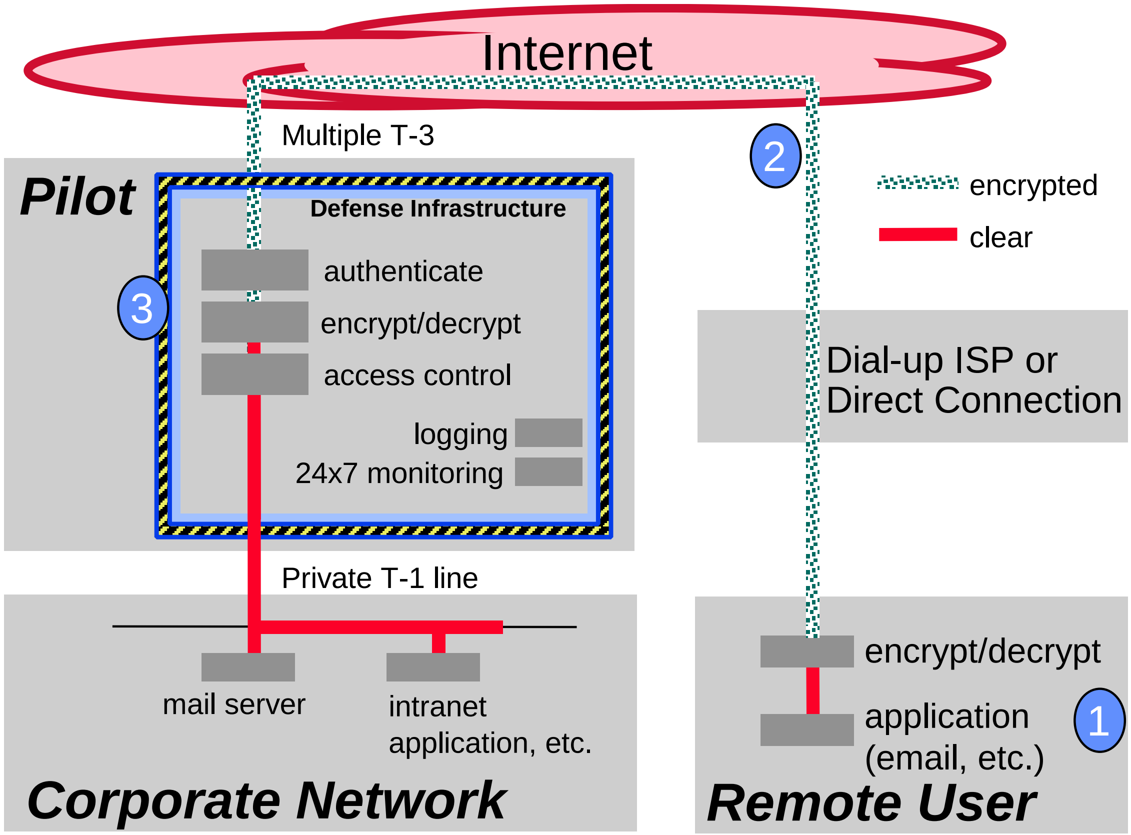

Figure 2: Pilot Secure Road Warrior Network Layout

Figure 2 shows the Road Warrior data flow. TCP/IP traffic leaving the workstation and destined for a protected host is transparently encrypted before leaving the workstation (step 1). It travels via any dial-up or direct Internet connection to Pilot (step 2). The traffic passes into Pilot's Heuristic Defense Infrastructure (step 3) and is authenticated and then decrypted. At no point is decrypted or "plaintext" data exposed to unauthorized viewers on the Internet. The Heuristic Defense Infrastructure enforces the specific security policy of the customer, controlling and monitoring access on a user-by-user, host-by-host, and application-by-application basis. The traffic continues on to the destination Intranet host. For more information on Authentication (Step 1), see Appendix A. For more information on access to the Internet (Step 2), see Appendix B.

Benefits

Cost Effective: Using the Internet for mobile telecommuters yields dramatic savings. Pilot's Secure Road Warrior leverages these savings and is transparent to the internal network infrastructure, requiring no internal network or server changes. Your networking staff continues to focus on their critical projects.

Scaleable: Unlike modem banks and channelized T-1 lines, a Secure Road Warrior solution scales gradually with usage. Total throughput depends on the volume of data across all users, independent of the number of connections. Throughput can be increased at any time by adding additional bandwidth between Pilot and your Intranet.

Flexible: Secure Road Warrior works with any TCP/IP application. Applications require no modification; the software operates completely transparently.

Reliable Worldwide: Telecommuters can arrange for their own Internet connections, or leverage Pilot's existing ISP roaming arrangements, enabling access from over 1,000 Points of Presence (POPs) in over 150 major cities worldwide. Network maintenance is no longer a support issue; if a certain local POP is busy or non-working, users simply try a different ISP in that city.

Secure: Secure Road Warrior leverages the same core Pilot security technologies and staff expertise which secure Pilot's other services, such as Secure Internet Connectivity and Secure Commerce Web Hosting. At the core of these services is the Pilot Heuristic Defense Infrastructure, monitored and upgraded continuously 24 hours a day, 7 days a week to defend against emerging attack techniques. The result, in the case of Secure Road Warrior, is a VPN solution tightly integrated with your corporate network security.

Integrated Solution: Encryption alone will protect data only while in transit; Authentication alone will protect against unauthorized intruders only; Static, fixed firewalls by themselves only limit traffic between certain hosts and applications. Pilot's Secure Road Warrior, on the other hand, provides comprehensive mobile telecommuting.

Pilot Secure Road Warrior enables mobile telecommuters to access internal corporate networks easily and cost effectively. Secure Road Warrior uses the Internet to carry traffic but all connections are fully secured: Data is encrypted in transit, and internal corporate hosts are protected from access by unauthorized users.

About Pilot

Pilot Network Services, Inc. is a leading provider of advanced Internet security for business. Pilot is the first Secure ISP and provides Internet security solutions through Network Security Centers nationwide, including secure Internet connectivity; Secure Telecommuting; secure Web, FTP, and News Hosting services; user authentication and encryption; Secure Road Warrior; and Corporate Partner Privacy. The Pilot Heuristic Defense Infrastructure is continually monitored and upgraded to maximize protection against intruders. Customers span a wide range of industries including software, hardware, biotechnology, telecommunications, financial services, retail, entertainment and transportation. Headquartered in Alameda, Calif., the privately held company has Network Security Centers in the San Francisco Bay Area, Los Angeles, New York and Chicago.

Secure Road Warrior Summary Specifications

Authentication: Two-factor RSA user/workstation authentication, using password-protected shared secret (see Appendix A for more information on authentication).

Dial-up access: Secure Road Warrior supports any IP-based Internet connection, dial-up or LAN-based, through any ISP. Secure Road Warrior seamlessly supports worldwide ISP roaming, for local access at over 1,000 POPs (see Appendix B for more information on roaming).

Encryption: 1024-bit RSA public-private session key encryption; 128-bit Triple-DES session encryption; export strength of 56-bit DES is also available. The session key lifetime is configurable.

Exportability: Secure Road Warrior technology has received Department of Commerce export certification for US-headquartered companies redistributing to employees of overseas subsidiaries. This certification greatly streamlines the case-by-case license application process.

Performance: *Latency*, or the elapsed time for a packet to complete a round trip, is highly dependent on the Internet connection between the remote workstation and Pilot. Latency due to encryption/decryption is minor in comparison. *Throughput*, or the total amount of data that can be carried, is generally the available bandwidth between the corporate internal network and Pilot. This connection starts at a single T1 and is scaleable in T1 increments (T1 = 1.544 Mbps). Secure Road Warrior throughput requirements increase with the total volume of traffic, not the number of concurrent users.

Requirements: Internal hosts: Secure Road Warrior supports any TCP/IP based application on any platform. Remote workstations: Secure Road Warrior supports any TCP/IP based Windows 95 application over a dial-up or LAN-based Internet connection. Support for Windows NT is planned.

Appendix A: Secure Road Warrior Authentication

Authentication in Secure Road Warrior starts when the remote workstation is turned on. At startup time, the user is required to enter a password (which may not be saved). This password does not ever go over any network, but simply unlocks a locally-stored configuration file. This configuration file holds the public and private keys for the local and remote nodes that make up the VPN.

This approach yields several concrete benefits:

1) nobody can use the laptop to enter the corporate network without the password (if it is stolen from an airport gate, for instance).

2) nobody can capture the password by eavesdropping on the network connection, because it never goes over the network.

3) nobody can read, decode, copy or “tailgate” the connection because they do not have the private keys for the VPN. The private keys are never sent over the network and are always stored in encrypted form. Therefore, nobody without the laptop can enter the corporate network, even if they have the password.

Appendix B: Internet Roaming

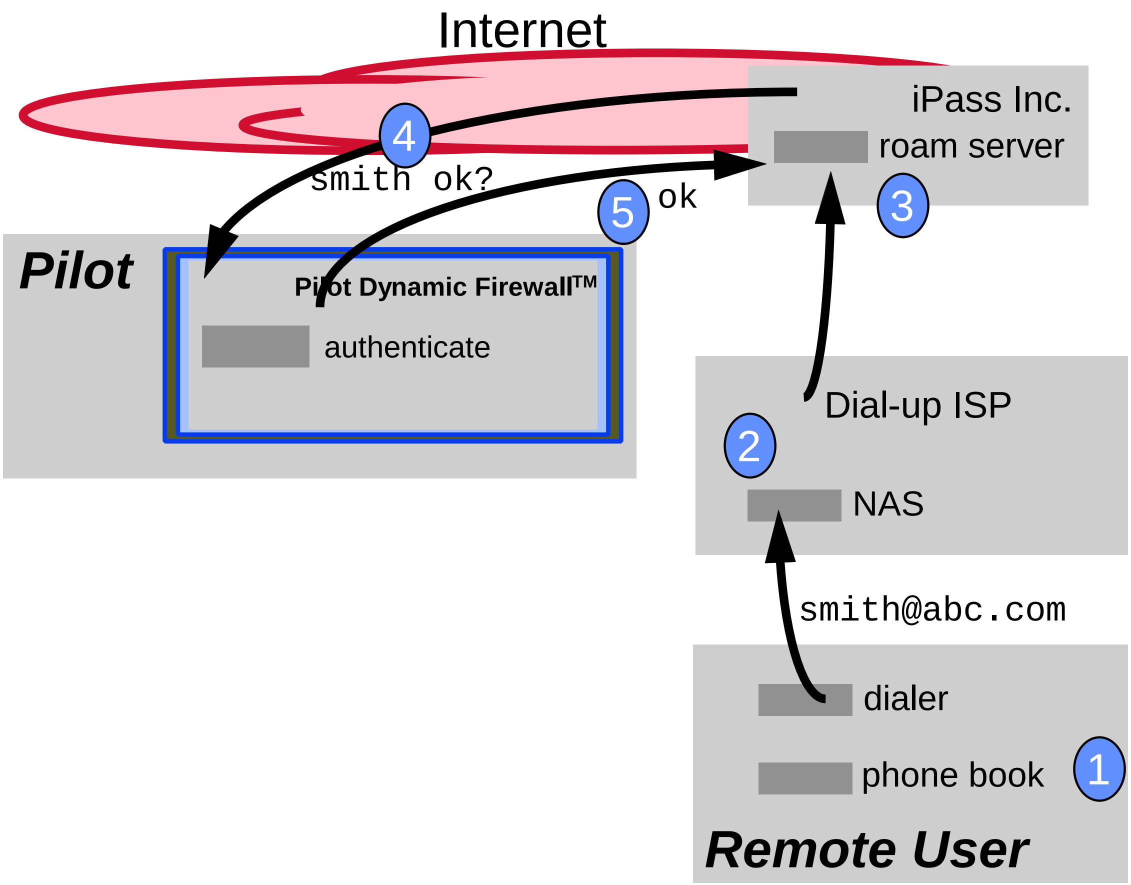

Figure 3: Internet Roaming diagram

In step 1, the user, arriving in a new city, uses the phone book to build a Microsoft Dial-up Networking Dialer. Networking parameters are set as well. The user then runs that dialer, providing their standard username, domain, and password. (step 2). The ISP reached receives the domain name and forwards it to iPass Inc., a roaming provider. (3) The iPass server recognizes the domain as served by Pilot and passes the username and password for approval. (4). Pilot checks the user and returns approval, which is forwarded to the local ISP (5). Connection is granted, and time is billed (rates vary by location). Secure Road Warrior works with any dial-up or direct Internet connection, including "flat rate" services. Roaming is not a requirement to use Secure Road Warrior.