



Pivot Point Security
957 Route 33
Suite 111
Hamilton Square, NJ 08690
(609) 890-1131
www.pivotpointsecurity.com



Lock IT Down: Consultant implements unique solution to meet customer's business and security needs

by [John Verry](#) | [More from John Verry](#) | Published: 6/11/03
Category: System Intrusions | **Audience:** IT Consultant
Rating: 4.5 (out of 5) [Rate it](#) **Comments:** 6 | **0 NEW** | [View all](#)
Takeaway:
Learn one consultants tricks to security

As a security firm, my company, [COUR.IT](#), often struggles with finding a reasonable and acceptable level of security to meet a broad range of business requirements. One recent engagement proved especially challenging: We were tasked with securing a business-critical database for a purchasing cooperative, while making it widely accessible to a mix of business partners and vendors without using virtual private networking (VPN) as part of the solution.

Here's a look at the unique business requirements that drove this situation and how we used a new technology to architect a solution that exceeded the client's expectations.

A new technology acronym

We were engaged by the business manager of "Client, Inc. (CI)" to secure the back-end database for a new Web application developed on its behalf. The business manager was extremely concerned about security because the database housed all of the pertinent and private information about the more than 500,000 members of its purchasing cooperative, along with their purchasing history of more than 4 million transactions.

He detailed two significant challenges: Share the data with a wide range of business partners and develop a solution that was "ACUI." My first concern was my lack of familiarity with the acronym. The business manager explained that ACUI stood for "AI Can Use It."

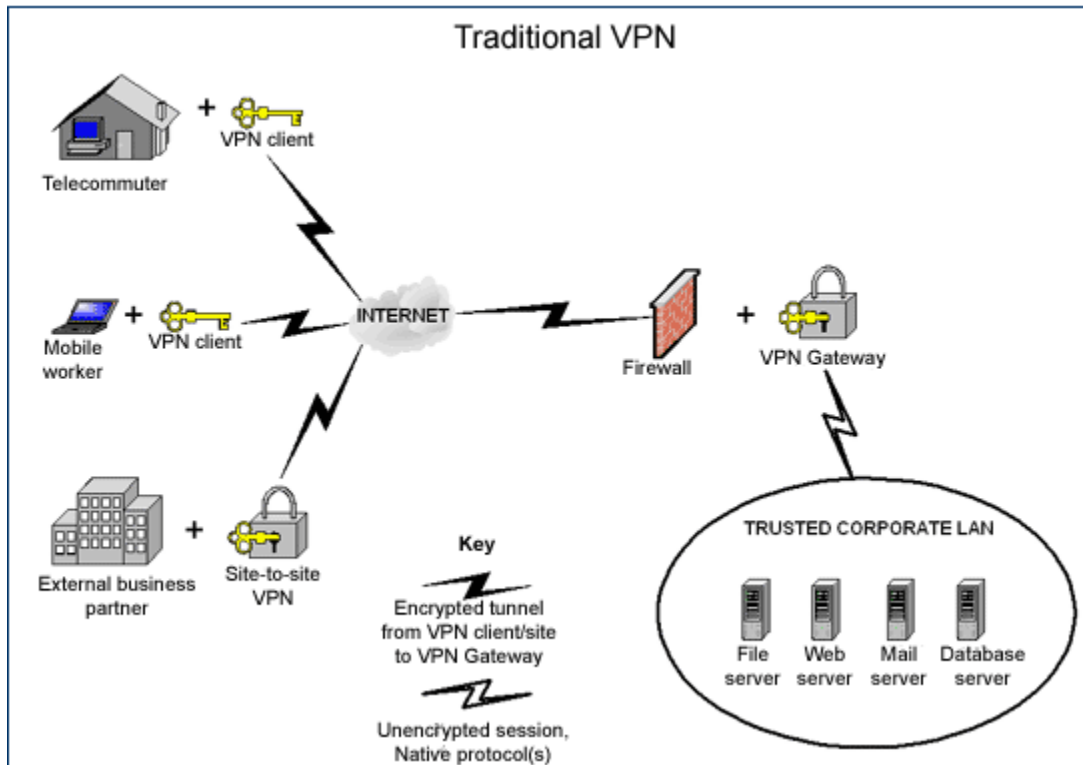
AI was the owner of the company and was hesitant about technology and change. For instance, before the company's Web application was developed, the company ran on the same mainframe solution for more than 20 years. AI was only willing to change when the index card-based solution he developed became too cumbersome to use with more than 100,000 members.

Driving nails without a hammer

ACUI, coupled with some of the more specific elements of the business partners' access, forced us to reconsider alternatives. We were dismayed that our security tool belt had an empty loop where virtual private networking usually sits (we sort of felt like a carpenter without a hammer). VPN technology has become ubiquitous in large part because it dovetails easily with most authentication schemes and allows data to be securely shared by remote users/locations when working across the Internet.

Figure A illustrates the setup of a traditional VPN solution.

Figure A



However, VPNs are not without their challenges. Most notably, VPNs require client-side software to perform the encryption/decryption that provides the "privacy" element of a VPN. In a perfect world, you install the software on any client machine that will be accessing your network, configure it appropriately, and forget about it. In practice, there are often client-side issues that can crop up for less technical end users, so it would be hard to propose a VPN-based solution as ACUI.

VPN paradox: Omnipresence complicates deployment

Paradoxically, VPN deployment becomes more difficult as the number of end users requiring client-to-site connectivity increases. This stems from the fact that most VPN solutions are based around proprietary client-side software. Proprietary software is not a problem if the intention is to deploy a homogeneous solution to a captive audience (for example, to employees for secure remote access). However, because CI wanted to deploy secure remote access to a broad array of business partners, this presented a major problem.

All users needing access to CI's data would need to install the VPN client software on their machines (site-to-site VPNs were impractical for CI). Unfortunately, many of the business partners had also deployed VPN solutions so the same users already had another vendor's proprietary VPN client installed.

We often find that loading multiple VPN clients on a single workstation invites disaster. (At CQUR IT, we use a Netscreen firewall and VPN. To support a customer, I also installed the Nortel Contivity VPN client on my laptop. After a failed installation, I found that I no longer had any TCP/IP capability. According to both vendors, my registry had been corrupted, with the only solution being to reformat the hard drive and start over. Ouch!)

Based on the ACUI factor and our inability to control the desktops of CI's business partners, we concurred that any proposed solution could not include VPN technology.

Something old, something new

Our company is a proponent of leveraging standard technologies and products. We find it simplifies implementation, allows higher levels of interoperability, and reduces ongoing costs. VPNs provide confidentiality by encrypting the data in transit across the Internet. Another technology that most Web surfers use to do the same thing is the ubiquitous Secure Sockets Layer (SSL) that is integrated into every major Web browser. Since SSL is proven (it enables most e-commerce transactions) and ACUI (even AI Can Use It), we sensed we were moving towards a secure solution.

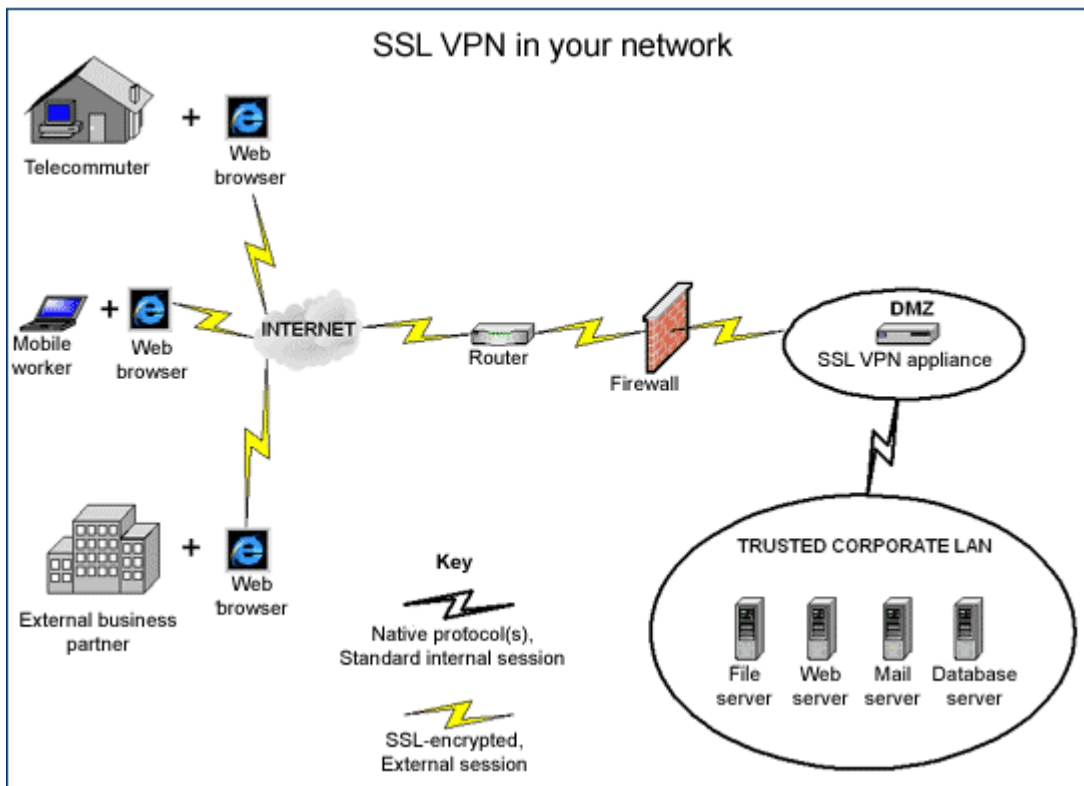
During the last six to 12 months, a number of vendors have introduced similar security appliances, which are often referred to as Instant VPNs, SSL VPNs, or Instant Virtual Extranets. In essence, they're hardened security appliances which, when installed in your network infrastructure (usually in the DMZ), allow end users to remotely access internal applications and data using the SSL inherent in their Web browsers to provide VPN capabilities. (Because these devices simplify the deployment, use, and ongoing support costs, many businesses are implementing them.)

At least 14 companies, including Neoteris, Aventail, and Netilla, are now offering SSL VPN products/services.

We selected the Neoteris product for CI because it provided out-of-the-box compatibility with the diverse range of application types (Web, Outlook, Telnet/SSH, client-server) that they sought to deploy. We also validated our decision against a recent Gartner report that placed Neoteris alone in its Magic Quadrant. Fortunately, the installation process was simple and we were able to fully implement the solution to all end users in half a day.

Take a look at **Figure B**, the SSL VPN solution we chose, and compare it to Figure A.

Figure B



Some of the advantages of our proposed solution included the following.

Reduced Total Cost of Ownership (TCO)

Savings are realized predominantly from the near absence of desktop support after deploying secure access to mobile employees and external business partners.

Increased security

Conceptually, the SSL VPN device is a proxy because it acts as an intermediary between systems/applications and end users. It terminates the end user's connection, establishes its own connection into the trusted LAN, and then returns the results to the end user. By eliminating open network-layer connections between the end user on the Internet and the corporate LAN, it greatly reduces the potential of being hacked by an internal user or a malicious outside user who gains access via the VPN.

Flexibility

The SSL VPN device is fully interoperable with all major remote access requirements (file shares, client/server applications, Outlook, Web) and authentication schemas/mechanisms (RADIUS, SecurID, etc.). Accordingly, all current and anticipated future needs could be fully met with this solution.

Benefiting from ACUI

While our organization works hard to maintain its knowledge of the IT security market, it is growing increasingly difficult as the market expands to encompass thousands of products. Projects like this one, that force us to reconsider the way we accomplish basic security objectives, are more difficult and time consuming, but they often provide a great opportunity to extend our knowledge and provide greater benefit to current and future clients.