

VPN or SSL-VPN

What Remote Access Solution is Right for You

By Don Faulkner, CISSP



www.safenet-inc.com

Approximately 40% of those surveyed in a survey of more than 50 users of IPsec (Internet Protocol Security) VPNs in Europe and the United States felt they had not achieved the expected cost-benefits of using a VPN, while a similar number felt their overall expectations were not fulfilled.

Most of the companies surveyed stated they were using VPNs for relatively basic applications, such as network file, CRM, and email access. Use of VPNs for more complex applications, such as voice data integration, automated two-way communication and extranets, remains a low priority.

Finding a cost-effective and secure way to give employees access to corporate resources with maximum uptime is a problem IT managers face daily. As more employees take advantage of wireless technology and the need to enable access to partners increase, secure remote access and stronger authentication becomes even more critical. There are a number of approaches to deploying a remote access solution – dialup is a widely used solution, but even small companies can receive bills for thousands of dollars per month to provide dialup service to employees. Companies are starting to utilize the Internet and secure VPN tunnels for remote access connectivity are the standard; either as a new service or to replace and augment expensive dialup solutions. Until recently, VPNs were given a great deal of press, but SSL-VPNs are quickly evolving as the leading technology for secure remote access and to help companies move away from expensive leased lines

This business white paper outlines potential issues and costs involved with deploying a dialup, VPN and SSL-VPN solution. It suggests that, in most cases, an SSL-VPN, can address most of these issues and may render a far lower total cost of ownership. This white paper concludes with an ROI analysis for a hypothetical one thousand-person company.

Dial-Up

Dialup has been the traditional way of providing access to corporate resources but is an extremely costly proposition. If providing remote employees with a toll-free 800 number, costs range from \$.10 to \$.25 per minute per connection.

Security problems can also exist with user names and passwords when using dialup. If an employee shares his or her user name and password with friends or family, the monthly telephone costs can rise dramatically and the company may experience a security breach.

Dialup is prohibitively expensive for any large-scale rollout, and is not the most secure solution available.

VPN (based on relative cost of an employee to a corporate VPN configuration)

VPNs grew out of the need to facilitate site-to-site communications between branch offices, as well as to combat the increasing costs of dialup solutions. They enabled access to closed private networks through cheaper cable modem and high-speed lines. VPNs have received a lot of sales and marketing “hype,” as have many other network technologies, and have been considered one of the most secure methods for remote access to corporate networks. However, issues associated

with VPNs are numerous. From a security standpoint, dealing with an array of sometimes-incompatible vendor products may be the deciding factor whether to use a VPN at all.

Using a VPN allows utilization of the Internet by tapping into the geographically distributed access that already exists. This offers greater scalability for VPNs, as it eliminates the need for an organization to continue adding the additional leased lines required for a dialup solution.

VPNs will also allow authorized users access to all the applications on a network to which they have been authorized access in the office. However, there may be additional access control configuration necessary at the firewall for each user's access control rules to be maintained. Most VPN deployments directly connect two networks and through this connection, tunnel users have access to exploit or launch vulnerabilities against multiple servers within the infrastructure.

When seeking a solution that is easily integrated with an existing network infrastructure, VPNs may not be the best choice.

A VPN Requires Deployment of VPN Clients

Desktop support can be burdened with issues during and after deploying a VPN. When deploying a VPN, the client machine must have the VPN client installed. Configuring VPN clients can present unique problems, because the VPN client interacts with the TCP/IP stack installed on the client machine. Updating and maintaining VPN clients for all users becomes both cost and resource-intensive.

IT may request that a laptop in the field be shipped back to headquarters for the computer to be configured with the VPN client simply because some of the problems that can occur during an installation are complex and difficult to troubleshoot remotely. VPN clients are fragile and can be a constant burden to desktop support to maintain deployed VPN clients.

With an IPSec VPN, users may have to manually enter an IP address and digital certificate settings. This adds complexity for the users as well as adding to the IT workload since IT usually ends up walking users through these processes. Odd problems can surface like a conflict with software drivers that control other communication or network adapter cards. To that end, desktop support, the network engineer and the IT manager may all expect additional support calls for the infield VPN users.

VPNs are designed for secure remote access over the Internet, yet there are some places where VPN connection problems are inherent. Users connecting from home may have to compromise their home network security in order to make a VPN client work. VPN clients cannot be installed on Web kiosks. A VPN connection may not be possible from a tradeshow, hotel room with high-speed access, or from a client site, as the network configuration is unknown. Particularly in a wireless hot spot connection, VPNs are vulnerable because everybody accessing the hot spot is using the same network. Once a hacker finds a computer that hasn't been patched, they have direct access into the corporate network using that computer's connection. Moreover, if the network configuration is known, additional firewall and NAT changes will likely be necessary.

The fact that VPN users often have to make complex individual adjustments to network configurations in order to make the VPN work is an indictment against the technology from the end user's perspective. Much of the design of IPSec was founded on the need to secure

communications between network sites. Its use for mobile user security, while reliable, is more adjunct functionality. As a result, the configuration adjustments that are relatively straightforward for network engineers are now required of the end user. This requirement alone should diminish the effectiveness of most VPN solutions.

SSL-VPN

SSL (Secure Socket Layer) is a means of protecting Web-based communications over the Internet at the application layer. SSL uses encryption and authentication to secure the communication between two devices, typically a Web server and client machine. With SSL, the applications (the Web browser and Web server) must support SSL. This is unlike IPSec, which operates on the network layer independently of the application. As most Web browsers currently support SSL, it is easy to deploy to a large number of users.

SSL raises the network security focus from the operating system level to the application level. Rather than functioning as an operating system service (which may require changes to the networking kernel), SSL uses the normal network protocols common to the Internet without change. As a result, it is completely portable between operating systems.

Supporting SSL at the Web server is the most complex task in deploying SSL within a network architecture. In addition to configuration of the Web server and obtaining SSL certificates, the added demands on system resources (CPU, memory) may overwhelm a heavily used server. This complexity is alleviated with the SSL-VPN, which provides the additional resources to support the SSL session and simplifies the deployment tasks. Because it utilizes SSL that is already built into each Web browser, there aren't complex or expensive clients to install or manage.

Previously, SSL-VPN appliances simplified the deployment of SSL within an organization, but lacked the ability to authenticate end users or to perform any kind of access control. A new breed of device, the SSL authentication gateway, addressed this shortcoming by providing SSL-VPNs with SSL termination and strong authentication through token-based authentication.

While SSL authentication gateways cannot provide the wide range of access that VPN technology affords, they can provide a level of protection to Web-based applications that VPNs cannot. In many circumstances, this is all that a VPN is used for; the additional capabilities of the VPN sit idle, waiting for a knowledgeable attacker to exploit them.

SSL-VPNs are the ideal solutions for organizations that want to provide Web-based access to internal information. The SSL-VPN protects the confidentiality and integrity of data as it traverses the network, and at the same time authenticates and authorizes users to access that data. Few, if any, changes are required—either on the servers or on the clients' systems.

Hardware Authentication Keys Versus Passwords

Password-based authentication presents a number of problems. Chief among these is that the compromise of a password often goes undetected. When a hacker guesses a password, the legitimate user is often unaware that his credentials have been stolen—that in effect, his or her identity has been stolen. Password sharing amongst users is a related form of this problem. Other

problems include the fact that passwords that are hard to guess are also hard to remember, resulting in additional administration costs to support users that have forgotten their passwords. Further, since passwords are hard to remember, the typical user often uses the same password in many locations: guess it once, and the hacker has them all. Not to mention, many passwords are written down, an obvious open invitation for any hacker.

Hardware authentication keys solve these problems by removing the user's interaction with the "password." Instead, users are issued a physical device that must be present for authentication to succeed. The device is often protected by a PIN code, similar to an ATM card, to prevent its use should the device be lost or stolen, establishing two-factor authentication. The hardware authentication keys themselves are difficult to compromise and almost impossible to share (without giving away the device itself). The hardware authentication key stores the user's "credentials" and since the user's secret resides on the key, he or she only needs their PIN to access the network. If lost or stolen, the key is useless to anyone. In fact, like the ATM card, it will lock up after a fixed number of incorrect guesses at the PIN.

Support for hardware authentication keys among VPN solutions have been sporadic and not usually easy to implement and support. In order to meet the increasing needs for this functionality, many SSL-VPN solutions already come tightly integrated with hardware keys

The Right Remote Access Situation, the Right Solution

A VPN is the best solution for site-to-site connections or if an enterprise is using only applications available through the network with no Web-based applications. Whether the enterprise chooses to use a software, hardware, or router-based VPN solution may be dependent on the resources and dollars available to support each solution. A software-based solution could require additional desktop support and may incur additional charges for equipment to be sent to IT headquarters for configuration. Hardware and router-based solutions could require the additional outlay of capital investment for the hardware appliances and both solutions need additional configuration, while the desktop support is virtually eliminated for these solutions.

An enterprise can greatly benefit by utilizing both VPN and SSL technologies with an SSL-VPN. SSL-VPNs secure access to both Web and non Web-based applications to employees remotely and within the corporate walls, as well as to partners, suppliers, and resellers. Today's leading SSL-VPN vendors enable full access to client/server and Web-based applications, as well as file sharing. Hardware authentication keys are integrated into the SSL-VPN, giving the additional security of two-factor authentication and eliminating the potential for brute force password attacks. Users requiring access to only Web-based applications could be granted controlled access via the SSL-VPN with the added benefit of two-factor authentication. Additional protection by isolating the Web server from vulnerabilities and protecting the Web applications from hacking, the SSL-VPN is worth an additional consideration. Deploying an SSL-VPN is an excellent consideration for an enterprise looking for ways to lower support costs.

A company deploying a new proprietary Web application for use by internal users, telecommuters and business partners should consider implementing an SSL-VPN and issuing hardware authentication keys to their business partners and users to protect remote access to their specific information and the confidentiality of that information. No additional changes are required to the

infrastructure other than granting appropriate access during the configuration of the SSL-VPN and the implementation of the hardware authentication key.

Often the simplicity of implementing and added protection of deploying an SSL-VPN solution can add weight to a decision of purchasing or migrating to the Web-based version of an application over a standard or enterprise version. There is also the added protection that the SSL communication tunnel closes when the identity token is removed from the client's computer closing the session immediately. SSL-VPNs extend security from the server all the way to the user

ROI Analysis: Dialup, VPN and SSL-VPN Solutions

In this analysis, total cost of ownership is computed over several months. In order to perform this, a determination is made regarding the initial expense for deploying such a technology. Because desktop, network support and line maintenance costs vary greatly, these additional costs have been omitted from the comparison. For the purpose of the analysis, a hypothetical one thousand-employee company that wants to remotely connect 400 users is considered.

Dialup Costs

Assumptions	
1000 total employees (200 use dialup, 400 use toll free 800)	
400 computer workers/telecommuters	
15 hours per week per employee	
\$.13 average cost per minute for toll-free 800	
\$19.95 per month Internet service	
400 workers x 15 hours/week x 60 minutes/hour x 4 weeks/month x \$.13	\$187,200
Investment	
Modems installed in employee PCs or laptops (cost not included)	
Ongoing Costs	
Modem maintenance (cost not included)	
Line maintenance (cost not included)	
Maintenance of dialup line authentication scheme	
Monthly cost of dialup (400 x \$19.95)	\$7,980
Average cost for implementing dialup	\$195,180
Ongoing cost per employee monthly (based on 1000 employees)	\$195.18

Considerations

- Modem and line maintenance is necessary for protection of core business protection. This ongoing cost has not been included in dialup costs.

VPN Costs (Hardware-based Implementation)

Assumptions	
1000 total employees (all users upgraded to broadband)	
400 computer workers/telecommuters	
Unlimited hours per week per employee \$45 per month broadband*	
Investment	
Expenditure for remote workers' equipment (client)	\$398,000
Initial outlay for VPN head equipment	\$22,000
Upgrade 400 users to broadband (400 x \$100)*one-time expense	\$40,000
Ongoing Costs	
VPN field maintenance (cost not included)	
Implement authentication mechanism to eliminate maintenance	
Broadband reimbursement (400 x \$45)*	\$18,000
Average cost for implementing VPN	\$478,000
Cost per employee to Implement (based on 1000 employees)	\$478

Considerations

- Modem and line maintenance is necessary for protection of core business protection. This ongoing cost has not been included in dialup costs.
- *Upgrade to broadband decreases long distance toll charges incurred with dialup and allows more long distance users for fewer dollars.
- Core business security behind configured firewall allows better protection than dialup modem and line maintenance.
- Redundancy of additional VPN equipment at \$22,000 is not considered.
- Payback period for initial VPN investment compared to dialup = 2.44 months.

SSL-VPN Costs

Assumptions	
1000 total employees (all users upgraded to broadband)	
400 computer workers/telecommuters	
Unlimited hours per week per employee	
\$45 per month broadband*	
Investment	
Initial outlay for SSL-based equipment	\$50,000
Upgrade 400 users to broadband (400 x \$100.00)*one-time expense	\$40,000
Ongoing Costs	
NetSwift iGate maintenance (cost not included)	
Broadband reimbursement (400 x \$45)*	\$18,000
Average cost for implementing NetSwift iGate	\$108,000

Cost per employee to **Implement** (based on 1000 employees) \$108

Considerations

- Rainbow Technologies' NetSwift iGate, an SSL-VPN 400-user configuration: \$50,000. Price also includes hardware-based keys for user license control.
- Redundancy of additional SSL-VPN at \$10,000 is not considered.
- *Upgrade to broadband decreases long distance toll charges incurred with dialup and allows more long distance users for fewer dollars.
- Key-based authentication and licensing is included with NetSwift iGate.
- Payback period for initial SSL-VPN investment compared to dialup = < 1 month.

Note: To increase the numbers allowing access to all 1000 employees, total cost of the SSL-VPN implementation increases to \$233,000, averaging \$233 per employee, still a substantial savings in comparison to a VPN solution.

Analysis

SSL-VPNs average \$108 per employee to implement. Hardware-based VPN implementation averages \$478 per employee and ongoing dialup costs at \$195 per employee for users accessing the toll-free 800 number. While the comparison being made bases SSL and VPN on implementation costs and dialup on ongoing service costs, the point is that the implementation costs have a payback period and are not ongoing. The assumption in the dialup analysis is that users are connecting to the company for an average of 15 hours per month, a conservative estimate. VPN and SSL costs assume unlimited access time and include the upgrade to broadband for all employees who require remote access.

No costs have been associated with support for line maintenance or client installation on dialup nor have costs been associated with the configuration of the hardware-based VPN installation. Both of these solutions would require numerous resource support hours for installation, configuration and maintenance.

None of the solutions have provided for redundancy requirements. While redundancy is not a one-step solution for backup equipment in the dialup arena, with the SSL-VPN, one additional hardware client (configured) would serve for VPN redundancy while an additional SSL-based appliance (configured) would fill the requirement for fail over.

Conclusion

Dialup is the most costly method to connect employees to corporate resources and is slowly being replaced with more cost effective solutions. Deploying VPNs requires modification to the current network infrastructure and may incur ongoing IT costs associated with maintaining a large number of VPN clients. Because of inherent problems, not all users will be able to effectively use VPNs. SSL is industry-proven at offering strong encryption for Web-based communications over the Internet. No matter the scenario, external access to sensitive internal information makes strong authentication a necessity. The past reliance on username and password for authentication is inadequate. Hardware authentication keys provide an additional level of assurance while simplifying the end user's tasks and lightening the administrator's load.

VPNs offer applications access to the end users that are available on the enterprise network. However, some firewall configuration may be necessary for the correct access control to these applications. VPN clients also require ongoing support from the desktop support group as well as continuous changes to the firewall to accommodate the user's current venue. VPNs will also require additional support to move to the two-factor authentication provided by hardware identification tokens. VPNs have traditionally been the best solution for non Web-based applications or those applications that require a two-way automated communication. Unfortunately, VPNs also carry risks for security breaches or vulnerabilities to the existing infrastructure.

Deploying an SSL-VPN offers an easy fit into an existing environment and provides for a quick, easy installation and configuration. There are no complex, intrusive clients to install, which leads to significant cost savings. Access control is truly enforced by extending access to the user, no matter where the user is and no matter which machine is used. Passwords are replaced with hardware authentication keys. No more simple passwords that can be guessed, and no more complex passwords to forget, write down or manage. An enterprise can benefit from using an SSL-VPN for its ease-of-use, scalability, integrated hardware key capabilities, low ongoing maintenance costs and a guarantee of connecting all users all the time. The savings combined with other appliance benefits makes the SSL-VPN the clear front-runner for secure access to both Web and non Web-based applications.

Reference

http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpcbn_wp.pdf

<http://specials.ft.com/ftit/sept2001/FT3TVDYX4RC.html>

<http://www.internetwk.com/VPN/supplement329-2.htm>

<http://www.networkcomputing.com/1123/1123ws2.html>

Rainbow Solutions

Rainbow Technologies is a leading provider of information security solutions for mission critical data, access control and software protection. Founded in 1984, Rainbow Technologies has been breaking the security paradigm by making complex security simple to implement and use for over two decades.

Rainbow Technologies provides a simple, secure, highly scalable, and cost-effective remote access solution with NetSwift iGate. NetSwift iGate protects access points all the way to the **user** with its "always on" SSL protocol, two-Factor authentication tokens, and access control. With NetSwift iGate you can have the balance of ease of use **and** higher security. For more information on NetSwift iGate, the most comprehensive SSL VPN solution, visit: <http://www.rainbow.com/netswiftigate>.



www.safenet-inc.com

Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: **+1 410.931.7500** or **800.533.3958** eMail: info@safenet-inc.com

Australia +61 3 9882 8322
Brazil +55 11 6121 6455
China +86 10 8266 3936
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852 3157 7111

India +91 11 26917538
Japan +81 3 5719 2731
Japan(Tokyo)+81 3 5719 2731
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore (1) +65 6274 2794

Singapore (2) +65 6297 6196
Taiwan +886 2 6630 9388
UK +44 1932 579200
UK (Basingstoke) +44 1256 345900
U.S. (Massachusetts) +1 978.539.4800
U.S. (New Jersey) +1 201.333.3400
U.S. (Virginia) +1 703.279.4500

U.S. (Irvine, California)
+1 949.450.7300
U.S. (Santa Clara, California)
+1 408.855.6000
U.S. (Torrance, California)
+1 310.533.8100

Distributors and resellers
located worldwide.

©2004 SafeNet, Inc.