VPN vs. RAS

How Virtual Private Networks (VPNs) Save Money and Improve Security

Tim Armstrong

December 1998 (Revision 1)

V-ONE® Corporation White Paper - © Copyright V-ONE Corporation 1998

The Evolution of Private Networks

A major objective of most IT departments is to gain a competitive advantage by providing their organizations with the most direct and cost-effective means of communicating with employees, partners, and customers (collectively known as communities of interest). In the past decade, there has been a steady evolution of infrastructure and security technologies designed to meet this objective.

In the 1990s, organizations have relied on private networking services for communicating with their communities of interest. Value Added Networks (VANs) were built to enable commerce with customers and partners. Wide Area Networks (WANs) have been the preferred way for connecting remote offices. Remote Access Service (RAS) was used to provide remote or traveling employees with LAN access. These technologies require proprietary circuits and/or long distance connections, making them costly to operate.

The emergence of the commercial Internet in the mid-1990s offered the potential for delivering the most effective means of communicating with worldwide communities of interest. The Internet’s global infrastructure presented an intriguing alternative to the more expensive VAN and WAN infrastructures and RAS implementations. However, before the Internet’s potential could be utilized, one issue still needed to be addressed – security.

In mid-1990s, LANs were secured with firewalls. Firewall technology allowed companies to connect and protect – connect to the Internet and protect company data assets from intruders. The firewall’s defensive design, at this time, did not support Internet-based remote access to protected networks. Database, mainframe, group ware, and Web applications that provide essential data for key business processes could not be deployed to remote users over the Internet.

With the absence of a security technology that enabled secure Internet-based business communications, today’s enterprise networking architecture was built consisting of a hybrid of VAN, WAN, and Internet networking (see Figure 1). The architecture has been segmented into private and public spheres, with perimeter firewalls representing the line of demarcation between the two. Private WANs and RAS servers provide private transport services for employee-based Intranet applications, while the Internet is utilized for outbound access and hosting public application servers. This segmentation of private and public wide-area network infrastructure increases costs and limits the scalability of enterprise applications.

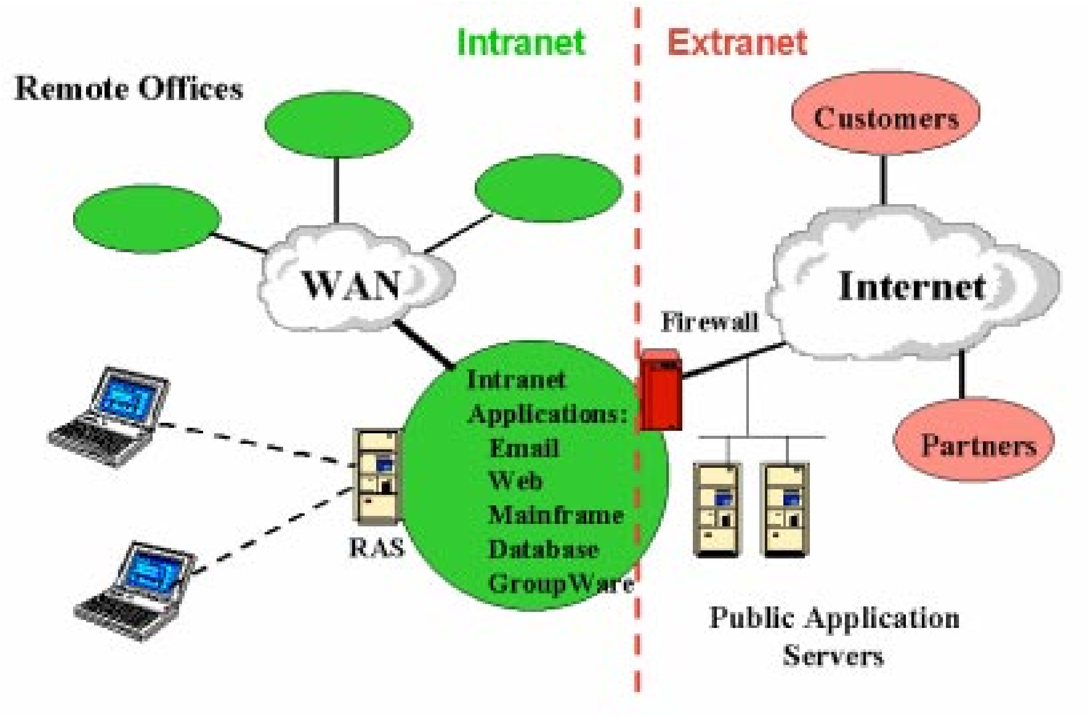

Figure 1: Today's Enterprise Architecture – Private and public segmentation increases the cost of infrastructure and adds complexity to application environments.

Virtual Private Networking (VPN) is the security technology that will enable organizations to leverage the Internet as a private enterprise backbone infrastructure. Much has been made of the value of intranets, extranets, and E-commerce, but until they can be deployed globally, using scalable network infrastructure, their impact will not be fully realized. Using VPNs, all application services hosted on the trusted enterprise can be targeted for worldwide communities of interest using the most cost-effective communications infrastructure available – the Internet.

Just how much money are organizations spending on RAS? According to Michael Howard, President of Infonetics Research, "An average of 18 percent of companies' entire IS budgets were spent on remote dial-up access solutions." And how much money can be saved by replacing RAS with a VPN? According to David R. Kosiur, author of Building and Managing Virtual Private Networks, cost savings can equal 50-75%. Later in this paper detailed cost comparisons are made between VPNs and RAS.

What Is A VPN?

A VPN can be defined as *a means for using public network infrastructures, such as the Internet, to provide private, secure access to applications and corporate network resources to remote employees, business partners, and customers* (see Figure 2). Migration from proprietary and private networking services cannot be achieved immediately or entirely. However, companies that exploit the cost-effectiveness and global reach of the Internet for delivering business applications to valuable communities of interest will rapidly gain a competitive advantage.

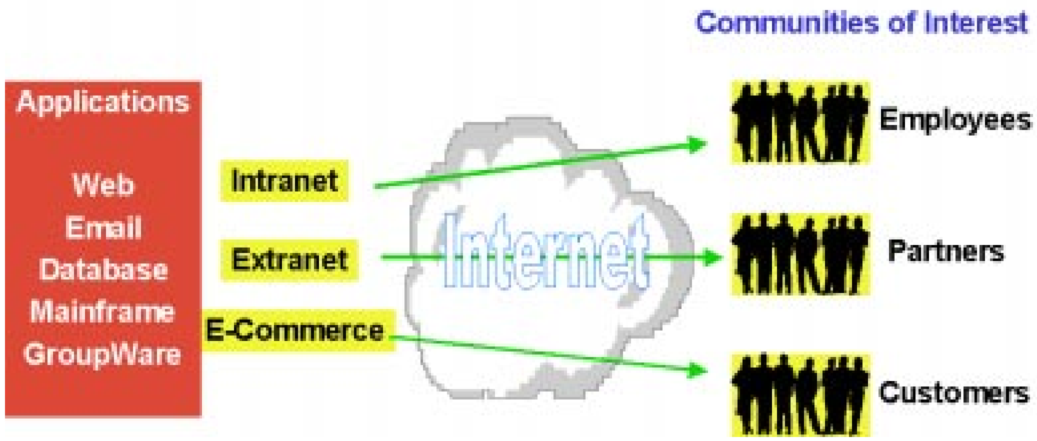

Figure 2: VPNs enable direct business communications with worldwide communities of interest by leveraging the Internet.

VPN Security Features

In order to ensure secure LAN access, a VPN needs to provide the following features:

- **Authentication** – Authentication is needed for both users (people or computers) and data. User authentication, to be done properly, requires a remote user to authenticate himself to a server and the server to authenticate itself to the remote user. This is known as mutual authentication. It prevents “man-in-the-middle” attacks whereby a third party attempts to impersonate the remote user or server. Data authentication provides assurance that a message has not been changed while in transit between the sender and the receiver.

- **Data Encryption** – Encryption scrambles information and makes it unreadable to anyone without the proper key. While the encryption process must be strong enough to ensure that private information sent over the Internet remains private, it must also be implemented in a way that does not significantly affect network performance. The procedure for distributing keys is also critical. It must be scalable in order to make using a VPN cost effective.

- **User Access Control** – Providing a remote user access to a private LAN does not imply the user should have access to the entire network. Different users have different needs, so their access privileges should be set accordingly. The ability to group users with common access needs is important to making this process manageable. Grouping users can best be accomplished with detailed control capabilities that enable permissions to be specified by destination host, connection service, or URL file name.

- **Event Logging** – In order to manage and audit a network, an events log is needed. This log should automatically record important events such as adding or deleting a user and session start and end data. One of the most important events to track is unsuccessful user logins. These can be studied to help determine if someone is attempting to attack the LAN.

Why Use V-ONE's SmartGate VPN vs. RAS

SmartGate VPN and RAS both serve the same purpose, providing organizational LAN access to remote communities of interest. However, there are important differences between these two technologies in performing this function, including:

- **Communications Costs** – Using SmartGate VPN, remote users place a local call to their Internet Service Provider (ISP) then connect to the organizational LAN via the Internet. Using RAS, remote users place a long-distance or toll call to the organization's modem banks in order to connect to the LAN. An ISP account costs about $20 per month for unlimited access while daytime long-distance calls can cost 25 cents or more per minute. The cost difference is substantial, and its significance grows over time or as the number of remote users increases.

- **Equipment Costs** – A SmartGate VPN server can be nothing more than a typical, Pentium II network server capable of handling about 50 concurrent sessions and cost $3,900, or it can also be loaded on an existing firewall computer. A 12-modem RAS server costs about $9,600 and a 48-modem RAS server costs about $15,600.

- **Personnel Costs** – VPN administration can be handled by mid-level IT personnel. RAS equipment requires additional expertise handling modem banks and solving telecommunications issues, and therefore needs a more specialized administrator.

- **Authentication and Encryption** – SmartGate VPN includes user authentication, data authentication, and encryption capabilities in its client and server software. The authentication methods mean users have verification with whom they are communicating and evidence if a message has been altered since the sender sent it. Encryption means information is securely transmitted preventing anyone except the intended recipient from reading it. RAS products often do not include these capabilities. Adding them would require integrating a third party's authentication and encryption products.

- **Access Control** – SmartGate VPN has an access control system which enables a system administrator to specify what each remote user has access to once connected to the organization's LAN. Remote users with similar needs can be placed into groups with pre-defined access privileges thus simplifying system management. RAS lacks an access control system, which means once users have LAN access, they can essentially use any application or service on the network.

SmartGate VPN vs. RAS Cost Comparison

Example 1

The first cost comparison illustrated is a real-world example using V-ONE Corporation during 1998. V-ONE has 16 remote offices and employees around the U.S. and abroad. Another 29 employees working at the corporate headquarters live far enough away that they would incur long-distance charges to access the HQ LAN. The following table shows the costs incurred by V-ONE to implement a VPN using its SmartGate VPN software and the potential costs it would have incurred using RAS.

The two most important differences between SmartGate VPN and RAS are the client/server software and the communications access. First, RAS client/server software does not include authentication, encryption, and access control capabilities available in SmartGate. This means that information is not secure during transmission. And second, SmartGate VPN enables remote users to make local calls while RAS requires remote users to place long-distance calls, meaning that SmartGate's communications costs are just a fraction of the RAS costs. By using SmartGate VPN instead of RAS, the total savings to V-ONE in 1998 will be about $59,174.

	SmartGate VPN	**RAS**
Client/Server Software	$9,450	(included with hardware)
Authentication Technology	(included in SmartGate VPN)	$2,700
Server Hardware	$3,900	$15,600
Internet Connectivity (T1)	$12,000	na
RAS Connectivity	na	$6,624
Network Administration	$20,000	$40,000
Communications Access	$10,800	$50,400
Total Costs	**$56,150**	**$115,324**

(An explanation of how these costs were determined can be found in the Appendix.)

Example 2

The second cost comparison is a hypothetical organization with 100 remote users over a three-year period. As mentioned previously, the greater the number of remote users and the longer the time period, the more impact communications access charges have. This hypothetical organization could save itself about $450,677 over three years by using SmartGate VPN instead of a RAS solution.

	SmartGate VPN	**RAS**
Client/Server Software	$12,895	(included with hardware)
Authentication Technology	(included in SmartGate VPN)	$6,000
Server Hardware	$5,100	$15,600
Internet Connectivity (T1)	$36,000	na
RAS Connectivity	na	$19,872
Network Administration	$60,000	$120,000
Communications Access	$72,000	$475,200
Total Costs	**$185,995**	**$636,672**

(An explanation of how these costs were determined can be found in the Appendix.)

Neither of these examples includes other, less-objective operational costs incurred with either VPN or RAS systems. For instance, cost of deployment. SmartGate VPN allows the client software and authentication tokens to be deployed over the Internet at a minimal cost. RAS client software can be deployed electronically; however, it does not have built-in authentication. A third-party physical authentication system for RAS needs to be set up and prepared for deployment, and the tokens must be delivered, either in person or via mail, to the end users. Thus deployment costs for RAS are several times as expensive.

On-going support for deployed systems is another issue. An organization’s people and equipment are continually changing. When new people need access or current users receive new equipment, they can use a Web browser and the Internet with SmartGate VPN to obtain their software and tokens. Using RAS, the tokens must be given to the user either in-person or by mail. Thus, on-going support for RAS has a much higher cost than does the support for SmartGate VPN.

Conclusion

SmartGate VPN enables organizations to provide remote users with LAN access both cheaper and safer than RAS can. SmartGate VPN users can take advantage of the Internet to make local calls for access to an organization LAN, but RAS users must make long distance calls to get access. Information sent over a VPN is secure, it's both authenticated and encrypted, while information sent via RAS lacks these security features. Although RAS served a purpose in providing LAN access to remote users, its time has clearly passed.

Appendix

Example 1 Costs

Client/Server Software

VPN – 45 users x $99 per user = $4,455 PLUS Server software = $4,995 EQUALS a total of $9,450[1]
(V-ONE used it's own SmartGate and SmartPass products and did not actually pay for these items.)

RAS – Included in cost of server hardware, however, typical RAS systems do not include authentication, encryption, or access control capabilities

Authentication

VPN – SmartGate VPN, unlike some VPN products, has built-in authentication

RAS – 45 users x $60 per user (renewable license, three-year minimum) = $2,700[2]

Server Hardware

VPN – Pentium II computer with 128 MB RAM[3]

RAS – 48-modem remote access server[4]

Internet Connectivity

VPN – 1 T1 line x $1,000 per month x 12 months = $12,000[5]

RAS Connectivity

RAS – 24 phone lines x $23 per line x 12 months = $6,624[6]

Network Administration

VPN – VPN management, $20,000 per year[7]

RAS – RAS management, modem bank management, telecomm management, $40,000 per year[7]

Communications Access

VPN – 45 users x $20 month for ISP connection x 12 months = $10,800[8]

RAS – 16 remote users x $0.11 per minute daytime long distance x 60 minutes per work day x 240 work days = $25,344 PLUS 29 corporate remote users x $0.10 per minute evening long distance x 180 minutes per week x 48 weeks per year = $25,056
EQUALS a total of $50,400[9]

Example 2 Costs

Client/Server Software

VPN – 100 users x $79 per user = $7,900 PLUS Server software = $4,995 EQUALS a total of $12,895[1]
(V-ONE used it's own SmartGate and SmartPass products and did not actually pay for these items.)

RAS – Included in cost of server hardware, however, typical RAS systems do not include authentication, encryption, or access control capabilities

Authentication

VPN – SmartGate VPN, unlike some VPN products, has built-in authentication

RAS – 100 users x $60 per user for three years = $6,000[2]

Server Hardware

VPN – Dual Pentium II computer with 256 MB RAM[3]

RAS – 48-modem remote access server[4]

Internet Connectivity

VPN – 1 T1 line x $1,000 per month x 36 months = $36,000[5]

RAS Connectivity

RAS – 24 phone lines x $23 per line x 36 months = $19,872[6]

Network Administration

VPN – VPN management, $20,000 per year[7]

RAS – RAS management, modem bank management, telecomm management, $40,000 per year[7]

Communications Access

VPN – 100 users x $20 month for ISP connection x 36 months = $72,000[8]

RAS – 100 remote users x $0.11 per minute daytime long distance x 60 minutes per work day x 240 work days per year x 3 years = $475,200[9]

End Notes

1. SmartGate price on 10/30/98.
2. SecurID price on 10/30/98.
3. Dell computer price on 10/30/98.
4. Ascend server price on 10/30/98.
5. MCI line price on 10/30/98.
6. Bell Atlantic line price on 10/30/98.
7. Based on partial time of salary for network administrator 10/30/98.
8. Typical ISP price on 10/30/98.
9. AT & T long-distance price on 10/30/98.