



Finding Your Way Through the VPN Maze

MAKING SENSE OF THE EMERGING VIRTUAL
PRIVATE NETWORK MARKET

Table of Contents

| | |
|--|----|
| Introduction | 2 |
| Entering the Maze: Major VPN Usage Scenarios | 4 |
| Intranet VPNs (Site-to-Site: a server-to-server application) | 4 |
| Extranet VPNs (Business-to-Business: a server-to-server applications)..... | 5 |
| Remote Access VPNs (Network controlled access: client applications)..... | 5 |
| Internal VPNs (Internal communications: client-to-client)..... | 6 |
| Into the Maze: Major VPN Alternatives and Solutions | 7 |
| Dedicated Hardware VPN Servers | 8 |
| Router Based VPNs VPN Servers | 9 |
| Firewall Based VPN Servers | 9 |
| Software Based VPN Clients..... | 11 |
| The Network Associates Solution..... | 12 |
| Summary | 14 |
| Appendix..... | 15 |
| Common VPN Standards | 15 |
| Encryption | 15 |
| Authentication | 16 |
| Tunnel and Transport Modes | 17 |

The information in this white paper has been provided by Networks Associates Technology, Inc. To the best knowledge of Network Associates, these companies offer the types of products described. These companies are solely responsible for their software, distribution, and support services. Network Associates disclaims any and all liabilities for and makes no warranties, expressed or implied, with respect to these products, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose. Distribution of these products, or information concerning these products, does not constitute Network Associates' endorsement of the products, the companies, or support services. Product information is subject to change without notice.

Introduction

In just a few short years, Internet connectivity has literally changed the way the world does business. Until recently, the Internet played a valuable, but largely passive role in most organizations. To remain competitive in today's marketplace, however, companies of all sizes are rapidly moving core business functions to Internet-based technologies.

Conducting business on the Internet is made possible, in large part, through the emergence of robust, standards-based Virtual Private Networking (VPN) products. By encrypting and authenticating all communications, VPNs give organizations a secure and cost-effective way to use the public Internet for even the most confidential and mission-critical applications. When properly implemented, VPNs effectively extend your secure private network to remote users, distant offices and external business partners at a fraction of the cost of leased lines. For the cost of a local connection, VPNs allow an extended enterprise to conduct business over the Internet securely from anywhere in the world.

Unfortunately, the emerging new VPN market can be extremely confusing. Organizations looking to make a sound business decision are faced with complex technology concerns, interoperability problems and conflicting messages from a wide range of both software and hardware vendors. Whose VPN solution is right for you? Should you buy from your network equipment vendor? From your firewall vendor? From a dedicated VPN provider? Is a dedicated hardware box the right approach, or will a software product provide

a better solution? If you combine solutions from different vendors, will they work together?

All too often, VPN buyers must struggle through a confusing “maze” of datasheets, vendor promises and dead ends.

This paper was written to help make sense of today’s VPN market for business decision makers. We begin by segmenting the most common usage scenarios for VPN products in today’s e-business environment. Next, we examine the four primary categories of modern VPN products, discussing the pros and cons of each. Finally, we conclude with an overview of the PGP VPN solution from Network Associates and where it fits in today’s marketplace.

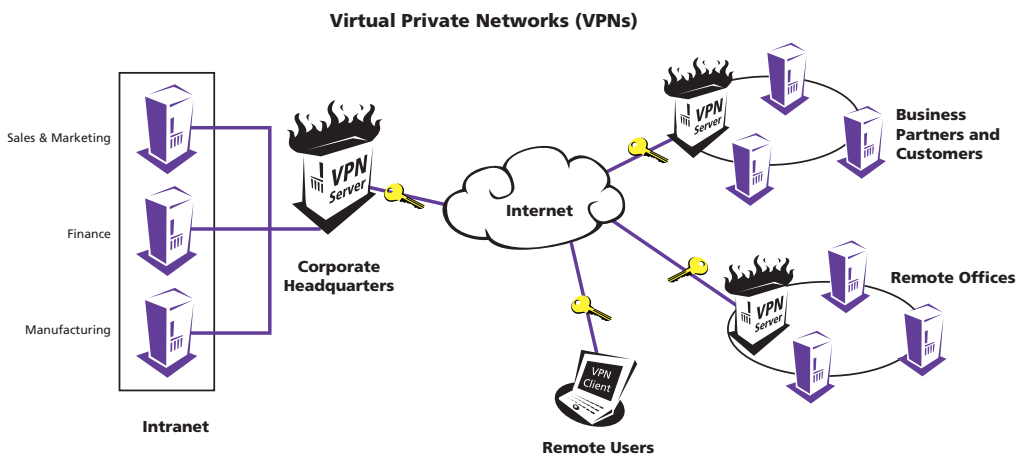


FIGURE 1

VPNs allow organizations to securely and economically expand their network boundaries.

Entering The Maze: Major VPN Usage Scenarios

When aspiring to improve costs, enhance security, or expand connectivity you'll be working your way through the VPN maze created by a large selection of solutions offered by multiple vendors. To make sense of this maze, you must first consider how you plan to use VPN technology and what benefits you expect to gain. The most popular options are:

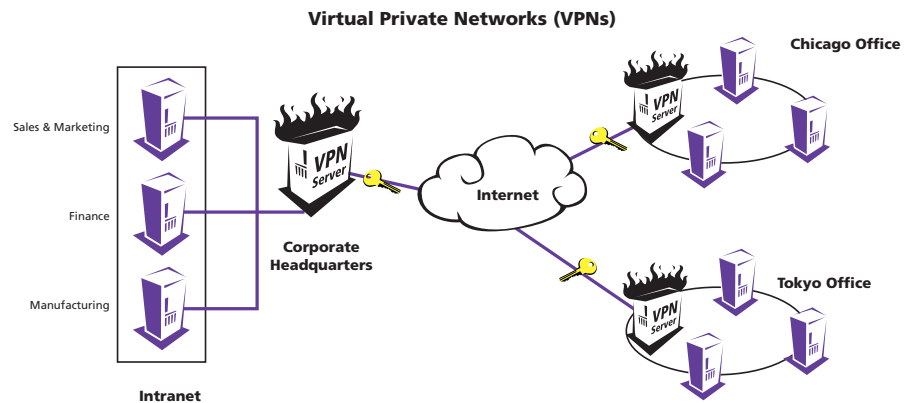
- An intranet, or site-to-site VPN, linking remote sites and/or branch offices
- An extranet VPN, interconnecting your business partners and customers
- A remote access VPN, linking mobile and remote employees to your central network
- An internal department-to-department or client-to-client VPN, securely connecting in-house users who transfer sensitive or restricted information

Intranet VPNs (Site-to-Site: server-to-server applications)

Connecting branch offices together typically results in expensive leased line long distance charges or frame relay connections. Establishing a site-to-site VPN between offices can result in tremendous cost savings by extending your existing Internet link to include

FIGURE 2

Intranet VPNs allow companies to connect multiple offices far more efficiently than through expensive leased lines.



secure site-to-site networking. As a result, you no longer require two separate connection points - one for connecting distant sites and one for connecting to the Internet. The bottom line is an immediate return on your investment (ROI) by eliminating long distance charges and excess capital equipment.

Sometimes, connecting sites will involve high-volume traffic moving between trusted endpoints. You will want these connections to be transparent to internal users. With an intranet site-to-site VPN, therefore, interoperable high-speed connectivity will be a priority. Since you are moving information between trusted parties, providing greater levels of access control, security will be less of a concern. High capacity routers and/or high-speed firewalls

with VPN functionality to your network perimeters are the most common solution for trusted site-to-site connectivity. Security requirements for intranet VPNs are typically limited to the strength of the encryption and authentication methods between your router or firewall connection points.

In some site-to-site cases, you may be concerned about protecting confidential information from intrusions or compromise. For these cases, user-specific authentication reaching beyond network perimeter points, all the way to the end user. VPN client software may be added to intranet VPNs for both encrypting and authenticating data all the way to your user endpoints.

Extranet VPNs (Business-to-Business: server-to-server applications)

Connecting your suppliers, vendors, distribution partners, and customers through extranet VPNs offers tremendous cost-efficiencies and e-business market opportunities. Because extranets involve sharing part of your internal network with external parties, security is a top priority. Supply chain extranets, in fact, often include multiple competitors within the same industry, further enhancing security concerns. Interoperability is another key requirement because extranets by definition typically require connecting multiple platforms, protocols, encryption methods, and authentication schemes.

With an extranet VPN, integrating your perimeter and end user solutions is necessary to guarantee tight end-to-end security. VPN enabled routers or high-speed firewalls in conjunction with robust VPN client software is often the best solution for shared extranet connectivity.

Remote Access VPNs (Network controlled access: server-to-client applications)

What are the methods you use for remote access today? Is it an 800-number that charges \$0.10 to \$0.20 per minute? Is the remote user that accesses your network fully authorized with strong digital authentication? With VPN remote access solutions, you can

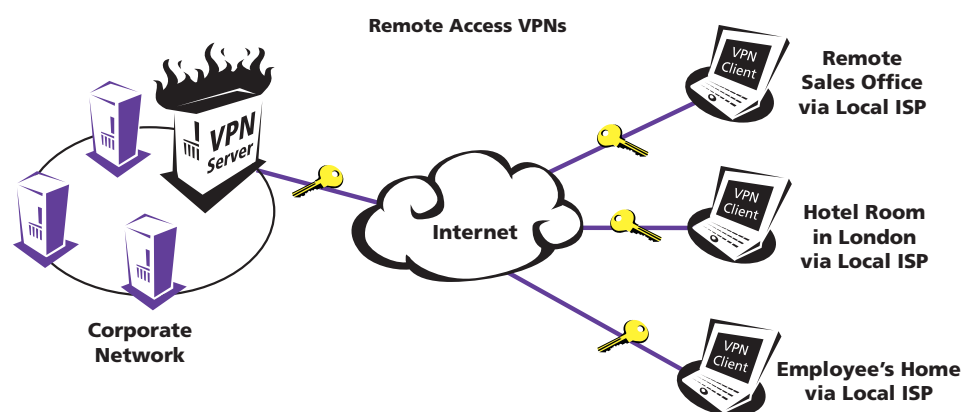


FIGURE 3

Remote access VPN solutions offer cost savings of 60-80% by allowing employees to securely access the corporate network through cost-effective local ISPs.

secure and authenticate both the users and the computers accessing your network. In addition to delivering secure network access, cost savings are immense. As a result, most organizations are moving away from traditional high-cost modem pools and leased lines to remote access VPN solutions. After a VPN server component is in place, the most critical element of a remote access solution is the VPN client software application. For secure remote access VPNs, ease of client use, ease of deployment, security, and manageability are all essential considerations. In addition, features such as interoperability, administrative pre-configuration of client, transparent interfaces, and silent installs will all be of critical importance during deployment.

When extending your corporate network out to remote users, VPN client software is what brings robust security out to the end user through strong encryption, authentication, and key exchange methods. When deploying VPN client software to the mobile user, other remote security requirements should also be considered such as securing sensitive files in case of laptop theft.

Internal VPNs (Internal communications: client-to-client)

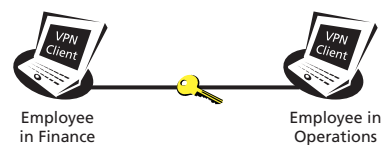
Despite the obvious requirement to protect external Internet transactions, the majority of security incidents still arise from inside organizations. The 1999 CSI/FBI Computer Crime and Security Survey reports that unauthorized access by insiders rose for the third straight year. Nearly 70 percent of all security breaches today, in fact, originate from internal employees or contractors.

Using a VPN solution, you now have the means to transfer data securely and effectively between departments and clients. Network access to directories and files can now be logged. The VPN client software protects data by encrypting and authenticating it all the way through your network to its end-points. For instance, human resources and payroll can now safely exchange salary information without the risk of a contractor or disgruntled employee gaining access to confidential data.

FIGURE 4

Nearly 70% of all unauthorized access today comes from within the organization. VPN technology can dramatically decrease this threat by securing all your network traffic transparently.

Corporate Internal Network VPNs



To avoid unnecessary expense and complex configuration issues, you should look for VPN clients that support direct, peer-to-peer interaction without routing connections through an intermediate VPN server or firewall. For cost effectiveness and efficiency, you will want to choose VPN client software with simple installation procedures. With broad deployments and wide spread operations, a client requiring little or no user involvement will save you a lot of money, as well as a lot of headaches.

Into The Maze: Major VPN Alternatives and Solutions

Now that we've looked at most common VPN usage scenarios, let's turn our attention to the various types of VPN hardware and software products on the market today. In this rapidly evolving market with so many vendors offering conflicting messages, it can be difficult to select which VPN solution is a best fit for your particular scenario. Understanding which vendors are providing which types of product solutions—including the features, advantages, benefits, and availability of the solutions—is a good place to start. Broad PKI support is also an important consideration, as is support of all interoperability standards. The four major VPN technology categories include:

- Dedicated hardware based VPN servers
- Router based VPN servers
- Firewall based VPN servers
- VPN client software

VPN servers provide for secure server-to-server networking through public networks. All VPN servers require VPN client software to enable secure communications to client end-users. For each category above, we will address the following questions:

- 1) What problem or need does this category of VPN products solve?
- 2) Who are the some of the vendors and what are their VPN products in this category?
- 3) What are some common usage scenarios for this category of VPN products?
- 4) What are some major pros and cons to consider when evaluating each alternative?

There are many technologically mature VPN server options on the market today. Fully functional VPN client software, by contract, is a relatively new market entry. Most VPN clients available today fall far short of market expectations for interoperability, transparency and ease of deployment.



Dedicated Hardware—VPN Servers

VPN technology itself began in the telecom world, when, companies like MCI began channeling private long distance telephone services through newly unrestricted telecom networks. In the data-networking world, VPN technology began with dedicated hardware-based VPN server companies offering early adopters a means to channel their WANs through the Internet at lower costs.

Dedicated hardware based VPN boxes typically sit in front of your network servers and provide for site-to-site (box-to-box) VPN connectivity. These dedicated boxes encrypt and authenticate the network traffic between them, passing the data then to the network server. Dedicated hardware VPNs do not provide VPN connectivity to the client; you still will need to add client software to bring VPN technology to the end-user. This is the case in all VPN based solutions for servers; you will always require client software to reach the end-user securely and effectively.

Vendors and Products

Leading vendors participating in the dedicated hardware based VPN server market include Radguard, Redcreek, Intel (Shiva), Timestep, and VPNet. The table at left shows you their respective products.

Usage Scenarios

Dedicated hardware VPN servers work well for connecting a simple intranet site-to-site VPNs. Vendors optimize these boxes for good VPN performance to secure traffic to and from the networked sites. These boxes work well carrying out redundant, large volume traffic processes that require secure communications. A perfect example would be networking two or three manufacturing sites from the same company together.

Evaluation

The main advantages of dedicated hardware VPN servers are that they are simple to install and to implement into existing networks, typically plugging-in, or sitting in front of your network. Dedicated hardware based VPNs are typically less valuable for remote access solutions, or any communications requiring multiple access privileges and security policies. They frequently do not handle multiple platforms, upgrading, or scaling well. These boxes typically require a separate purchase and the additional management of a firewall. In all cases, of course, client software is required for remote areas. One notable exception is the new *WebShield E-appliance* product line from Network Associates, which represents a new type of hardware VPN alternative by combining a VPN server, firewall and anti-virus scanner in a single device.

DEDICATED HARDWARE BASED VPN SERVER VENDORS

| VENDOR | PRODUCT |
|-------------|-------------|
| Radguard | CIPro |
| Redcreek | Ravlin |
| Intel/Shiva | LAN Rover |
| Timestep | Permit/Gate |
| VPNnet | VSU-1010 |

NOTE:

The new *WebShield E-appliance* product line from Network Associates represents a new type of hardware VPN alternative by combining a VPN server, firewall and anti-virus scanner in a single device.

If you have a simple site-to-site scenario appropriate for dedicated hardware based VPNs, be sure to pick one with high performance ratings and significant ease-of-configuration features.



Router Based VPNs—VPN Servers

Router Based VPN servers incorporate encryption and authentication routines into routers, giving them VPN functionality along with simple packet filtration capabilities. Most leading routers today now support VPNs, often embedding VPN functionality into the devices software set or operating system. As with all VPN servers options, a complete remote access solution to the end user, requires the addition of robust VPN client software as well.

Vendors and Products

Shortly after dedicated hardware VPN servers hit the marketplace, large networking vendors began extending the functionality of their routers to add VPN capabilities. Many routers today are now shipping with VPN functionality. Cisco, Lucent, and Nortel, for example, all include router based VPN technology in their product offerings.

Usage Scenarios

To meet the demands of high-volume traffic, many Internet Service Providers (ISPs) are using router based VPN servers. These VPN servers bring high performance, quality of service, and simple packet filtration to high-volume/low-level security scenarios.

Evaluation

Router based VPN servers can be a good fit for processing large volumes of traffic while offering basic security to the perimeter. Router based VPNs typically have simple packet filtration capabilities to determine where packets are coming from and where they are destined. These routers do not actually open packets to decide if they are a security risk. For this level of security you will also require a firewall.



Firewall Based VPN Servers

Firewall based VPN servers were created when security vendors began adding VPN security functionality to firewalls. Firewalls are a natural extension for VPN technology since the main purpose of a firewall is protecting your internal network through powerful access controls and other security features. Firewall VPN servers have extensive capabilities to effectively inspect all attempted connections at your Internet gateway. Combining encryption, authentication, and key exchange with existing firewall security features resulting in a robust and powerful VPN server solution.

FIREWALL BASED VPN SERVER VENDORS

| VENDOR | PRODUCT |
|--------------------|---------------------|
| Network Associates | Gauntlet VPN server |
| Check Point | VPN-1 |

Vendors and Products

Leading vendors supplying firewall based VPN servers include Network Associates and Check Point.

Usage Scenarios

Because of their easy manageability, robust security, and greater flexibility, firewall based VPN servers are the optimal choice for most corporate sites today. They work extremely well as an intranet site-to-site, extranet, and as a back-end for remote access client solutions.

Evaluation

With a Firewall based VPN server, you no longer require additional boxes or systems to provide robust VPN security to and from your network. Instead, firewall based VPN servers offer a one-solution alternative, enabling efficient central manageability and cost effectiveness.

The biggest benefit of firewall based VPN servers is additional access control and security. Their software base makes maintaining precious control over proxies, protocols, and standards a simple process. This allows for greater flexibility, security and manageability. Besides offering secondary authentication methods, firewall VPN servers, (especially those based on a proxy architecture) provide for more granular access control for managing tasks like remote-user authorization privileges. With proxy-based firewall VPN servers, you can even perform authentication to the application layer, securing traffic inside your network. With router based VPN servers, by contrast, authentication normally terminates at the network perimeter.

Recent innovations by the leading vendors have also brought tremendous improvements to firewall performance, boosting throughput up to 300% to make performance virtually a non-issue with newer firewall based VPN servers. Gains have come from new second-generation firewall architecture, (such as Network Associates patent-pending “adaptive proxy”) widely available load balancing solutions, and exponential increases in CPU performance. When evaluating firewall based VPN servers, look for products with a proxy-based architecture and built-in VPN functionality.

Quality client software is again necessary with firewall based VPN servers to provide complete VPN functionality to the end user.



Software Based VPN Clients

Software based VPN clients provide encryption, authentication, access control, and tunneling to the end user's desktop or laptop. These client systems give end users the power to connect to their servers securely from anywhere through the Internet at a significantly lower cost than traditional 800 line and modem pools provide. Some VPN clients also provide for secure peer-to-peer or department-to-department connectivity without the need for an intermediary gateway.

Vendors and Products

Leading software based VPN client vendors include Network Associates, IRE, Redcreek, and Timestep.

Usage Scenarios

Software based VPN clients are necessary in all VPN scenarios to provide effective functionality to the end user. The most common use of VPN clients is for remote access.

Evaluation

VPN client software is necessary to get secure connectivity to and from end users, and for complete end-to-end (client/server) VPN operations. Dedicated hardware, router, and firewall VPN products provide the server backend for large client deployments.

Don't ignore the importance of the VPN client when evaluating end-to-end VPN solutions. Many VPN server vendors are now beginning to offer low functionality VPN client software with their server products. Use due diligence when evaluating this type of client software if client software is often not the hardware vendor's core competency. *More VPN deployments fail because of weak client software than any other factor.*

Five very important attributes to consider when choosing VPN client software are:

- Proven security functionality protecting the network from end-to-end
- Pre-configuration and silent install for ease of deployment to remote users
- Easy transparent interface for ease of use
- Interoperability and support of standards like IPSec and IKE
- Built-in compression to reduce transfer time further and lower online costs

SOFTWARE BASED VPN CLIENT VENDORS

| VENDOR | PRODUCT |
|--|--|
| Network Associates | PGP VPN client |
| IRE | Safenet |
| Redcreek | RavlinSoft |
| Timestep | Permit |
| Large network equipment and firewall vendors | Various embedded "bare-bones" products |

Also, carefully consider a vendor's experience in delivering client software products when looking for a high-quality VPN client. You may also want to give close consideration to other security requirements at the desktop (e-mail security, file transfer security, laptop disk security, etc.), since managing multiple desktop security products can become cumbersome. *For most companies, the optimal solution is the combination of a robust VPN client with a proxy-based firewall VPN server.*

The Network Associates Solution

PGP VPN Client

Our end-to-end VPN solution begins with the PGP VPN client. PGP is the world's most widely used desktop encryption and authentication solution. PGP now boasts over 10 million users worldwide, and has been available commercially since 1991. By adding standards-based VPN functionality to the popular PGP client, Network Associates offers customers the most complete desktop client security on the market today.

The PGP VPN Client provides the following benefits:

- Full standard compliance with interoperability standards such as IPSec and IKE
- Certificate interoperability supporting both the X.509 and PGP standards
- Works with all standards-compliant VPN servers and firewalls
- The first VPN client supporting client-to-client VPNs without the use of a VPN server
- Simple end user operation, including transparent user options
- Easy pre-configurable silent installs
- Powerful compression to further reduce the cost of transfer time
- The first secure virtual NIC client with both tunnel and transport modes
- Includes e-mail, file and disk encryption in a simple, easy to use client
- Proven product with over 10 million users worldwide

Gauntlet VPN Server and Firewall

For users who want superior site-to-site intranet or extranet VPNs, our award-winning Gauntlet comes standard with our powerful Gauntlet VPN server. Gauntlet, an early pioneer in VPN interoperability standards, was one of the first firewalls certified by the International Computer Security Association (ICSA). Because it is based on our patent-pending adaptive proxy, users get unprecedented access control security in one of the fastest firewalls on the market today.

PGP VPN Suite

For a complete end-to-end VPN solution, Network Associates customers may also chose our full PGP VPN suite. This powerful solution combines the PGP VPN client with our Gauntlet VPN server and firewall. For customers who do not already have an existing public key infrastructure in place, we also include our Net Tools PKI at no additional cost. Net Tools PKI is a complete X.509-based public key infrastructure that is remarkably easy to install and manage. This allows customers with large client populations to automatically manage individual user keys without additional investment or deployment headaches. All Network Associates VPN products also support other leading PKI and certificate vendors for easy interoperability.

Summary

Simply deciding how and where to use a VPN is the first step to finding your way through the VPN maze. Your choices included intranets, extranets, remote access, and internal VPNs. Your second step is deciding which VPN product categories fit your usage scenarios best. VPN servers provide site-to-site VPN connections and serve as a backend for VPN clients. Software based VPN clients extend VPN security and cost savings.

Dedicated hardware and router based VPN servers work well at moving routine data relatively quickly and securely among a limited number of sites. Router based VPN servers offer a flexible alternative when high security is not a requirement. Firewall based VPN servers provide the most flexible and secure backend for most corporate environments, providing more granular access control and authentication to the application layer for securing connections to your network. Whereas other server solutions require separate purchase and management from your firewall, firewall based VPN servers provide an all-in-one solution. Software based VPN clients work in conjunction with VPN servers to reduce costs further by bringing complete end-to-end security to the end user. Software based VPN clients are a critical component for secure remote access or for any other scenario where security to the end user is important. *For most companies, the optimal solution is the combination of a robust VPN client with a proxy-based firewall VPN server.*

At Network Associates, network security and performance are our core competencies and we proudly leverage this strength to bring you a full range of interoperable and fully standards compliant VPN products. Customers may chose either our PGP VPN client or our complete PGP VPN suite (PGP VPN client, Gauntlet VPN server and firewall, Net Tools PKI). We are the encryption, authentication, and key management experts for secure communications over your LANs, WANs, and the Internet. At Network Associates, we want to connect and link you all the way through the VPN maze from beginning to end. Now is the time to bring the secure, interoperable, and fully standard-compliant Network Associates products into your organization to achieve an immediate and a lasting return on your VPN investment.

Appendix

Many VPN alternatives exist. The right solution for your organizations highly depends on your unique requirements. Typically, a VPN includes encryption to conceal your data, authentication to validate your users, and transport or tunneling protocols to protect your information across public networks.

Essentially, your VPN must be capable of securely transporting data across a public network. To achieve this security, your VPN will make use of encryption and authentication to transport or tunnel your data through a public network. We describe each of these functions in detail below.

Common VPN Standards

Implementing VPNs across the Internet and other IP-based public networks depends on vendors, service providers, and other interested parties agreeing on standards through the Internet Engineering Task Force (IETF). The VPN standard today is IPSec, which adds strong security to TCP/IP networking. IPSec addresses encryption, key management, and authentication to ensure data integrity and privacy. The benefits of IPSec are interoperable, high quality security for IP and/or upper layer protocols.

User groups consisting of manufacturers and suppliers are strongly supporting IPSec. Security is a critical component of VPNs; especially those implemented over the Internet. Encryption delivers the “private” in virtual private networking, and a basic aspect of encryption is the management of keys. Ensuring that only a recipient with a proper “key” can decrypt, read, and process a message-the Internet Key Exchange (IKE) protocol provides for the authentication and control of these keys.

Encryption

Converting plain text into cipher text using algorithms, encryption makes data unreadable to everyone except the intended recipients. Only those possessing a key or a password and knowing the algorithm can decipher (or decrypt) the cipher text back into plain text. Because of their randomness, many newer cryptography techniques are nearly unbreakable.

Encryption scrambles data in a VPN before transmitting it over a wide area link, such as the Internet. Two critical aspects of VPN encryption are processing power to encrypt every packet and management keys to unlock secure data at each remote end. Encryption is an important element of Internet VPN tunneling applications.

Strong encryption standards include Triple DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) in Europe, and CAST. These standards include 64 bit cipher algorithm protocols, providing the means for 128-bit key lengths and greater, which are virtually impossible to break. Maintaining security for financial transactions, the banking industry makes use of 128-bit encryption. Weak encryption standards use less robust algorithms and shorter length keys.

Authentication

Authentication makes use of passwords, token cards, and information handshakes to protect outsiders from intercepting your communications. Passwords are the most common, but most basic of authentication techniques. The Internet Key Exchange (IKE) protocol provides for the most robust and secure authentication method.

IKE uses public-key encryption where each person gets two keys, one allowing you to encrypt messages and another allowing you to decipher messages. You publish your public key and keep your private key secret. Encrypted messages are sent to your public key address, which you can only decrypt using your private key. Cryptographic algorithms and key lengths determine the strength of the encryption. Security levels depend on key length and the frequency of key change. A 128-bit key length is considered very strong. There is solid proof that 128-bit keys provide adequate protection. In fact, it would take a military intelligence agency, with a \$1 billion dollar hardware budget, a millennia to search half of a symmetric key-space of a 128-bit key. It is infeasible that any attacker could decipher any key longer than 80 bits.

Authentication also is important in multi protocol IP tunneling, to make sure that tunnel peers can only connect with each other. The authentication found in IPSec provides packet-by-packet verification, which prevents access to the tunnel by unauthorized users. Different tunneling protocols approach the issue of authentication in different ways. For LAN-to-LAN tunneling under IPSec, authentication uses digital signature technology. Digital signatures allow for continuous authentication on a packet-by-packet basis, preventing “spoofing”, or having an outside host assume command of a tunnel. Other tunneling protocols verify tunnel requests before a connection is established. Once a connection is established, encryption authenticates the link.

Authentication technologies guarantee the identity and authority of the participants using passwords, challenge phrases, tokens, and X.509 certificates. A good VPN allows us to choose the authentication solution that matches your needs.

Tunnel and Transport Modes

In the IPSec tunnel mode, you can connect an End Station (ES) to an Intermediate Station (IS), or two (IS) devices, for a secure connection. In the IPSec transport mode, you can connect an ES source to an ES destination for an end-to-end secure connection.

Combining encryption, authentication, and encapsulation-VPN tunnels provide for secure, virtual point-to-point connectivity through the Internet or other public networks. With tunneling, you can confine your user traffic, prevent unauthorized access, and maintain user confidentiality. In this tunnel mode, the Authentication Header (AH) protects your entire inner IP packet, including your entire inner IP header.

By encapsulating encrypted packets within other packets, which carry Internet routable source and destination address, this mode hides original user addresses to maintain confidentiality. The enveloped packet communicates with hosts or subnets behind your secure gateway using these Internet routable source and destination addresses. In a sense, your firewalls and routers now act as proxy destinations for your tunneled traffic.

Encapsulation also gives you the means of transporting incompatible protocols across your VPN. The source packet that resides inside of the tunnel packet can be of the same protocol or of a completely different one. Therefore with tunneling, you have the flexibility to make remote connections to various servers operating off different protocols.

The transport mode enables you to communicate securely between peers without an intermediary gateway. This mode is also applicable for end-to-end security over host devices, providing protection to IP header fields and to upper layer protocols.



Who's watching your network

For more information on products, services, and support,
contact your authorized Network Associates sales representative.

CORPORATE HEADQUARTERS

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (408) 988-3832*
Fax (408) 970-9727

**Call for additional Worldwide Sales Offices*

Visit our Website



www.nai.com