Virtual Private Networking
A White Paper

White Paper
Mike Ellsworth
Senior Project Manager
US Systems
Fall, 1998

Table of Contents

Introduction

Security is an extremely important component in any applications architecture ACNielsen adopts. The GartnerGroup report, **The Industry Trends Scenario: Delivering Business Value Through IT**, from 30 April 1998 lists the following concerns for enterprises in 2003:

- *Key technology enablers*: application interoperability (interenterprise/intraenterprise); high-speed networks (ubiquitous/reliable); rapid AD; terabyte database management systems (DBMSs); inter-enterprise collaborative computing; **security**! **security**! **security**!
- *Business-technology truths*: continued hardware price/performance improvements (i.e., Moore's Law through 2010); IT infrastructure recentralization/value-chain decentralization; IT skills demand outpaces supply through 2005; explosive use of external services providers (ESPs) and business process outsourcers; IT architectures remain inflexible or difficult to integrate.
- *Business-technology myths*: building complex systems only gets easier; industry standards work!; recentralization means mainframes; Java solves everything; the Internet is the answer; bandwidth is free; components take over the world; disintermediation rules; value-chains remain static!

The threat of a security breach is very real. In a white paper by entitled **The Importance of Protecting Information**[i], technology consulting firm Whittman-Hart quotes a GartnerGroup finding that 64 percent of the estimated 250,000 people who've hacked into U.S. Department of Defense computer systems have gained access to unclassified information:

> In the past, it was safe to assume that attacks were more frequent on Defense Department computers than general business computers. However, with businesses seeking to reap the benefits of intranet and extranet computing, more thieves and vandals are targeting these newly exposed systems. Commercial enterprises are less forthcoming about attack rates and successes, but several recent studies indicate that most, if not all, of the Fortune 1000 companies have been attacked repeatedly in the past year. Even assuming a low success rate, these attacks represent tremendous potential for disrupting business processes.

With the growth of the Internet and networking in general, the threat cannot be taken lightly. Each of the alternatives examined in this paper is evaluated as to how well it meets industry-standard requirements for a complete security solution. Virtual Private Network provider Check Point says there are three critical components to a security solution:

- Security
  - access control
  - authentication
  - encryption
- Traffic Control
  - bandwidth management
  - server load balancing
- Enterprise Management
  - key maintenance
  - logging
  - auditing
  - reporting

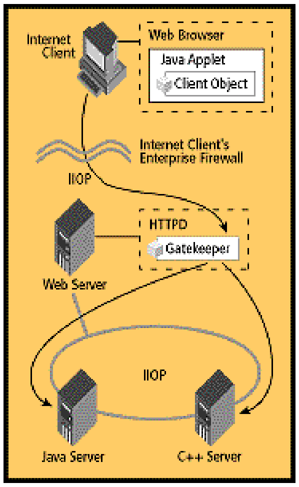
It is important to note that although only the first point appears to directly address security, in reality, all three points must be in place to have a comprehensive security solution. Security solutions should be evaluated with respect to satisfying these requirements, as well as:

- Firewall Issues A solution must take into account impacts on customer firewalls as well as the ACNielsen firewall. For example, not all protocols and communications ports are permitted to cross the typical firewall.
- Timing Impact on applications in the short and long term
- Cost Cost to implement, short and long term
- Risk A subjective assessment of the various types of risk imposed by the solution, both in terms of implementation risk, as well as risk of compromising enterprise security for customer and ACNielsen
- Support What will it cost to support the implementation? What challenges will ACNielsen face?

Visigenic Access Analysis

The current solution proposed involves using Inprise's Visigenic Gatekeeper and SSL Pack modules. It should be noted that other Visigenic components are in place, specifically their Object Broker, which provides CORBA communications services between the various application server components. These components are working flawlessly with the Visigenic components and no further work is required in this area.

The Visigenic Gatekeeper is an application proxy[ii]. According to Inprise, Gatekeeper "lets Java applets communicate with server objects across intranets and the Internet without compromising the network security. VisiBroker Gatekeeper serves as a gateway from an applet to server objects providing full client capabilities to applets traditionally constrained by firewalls or browser restrictions."



The user application binds to an object on the Gatekeeper using Internet InterORB Protocol (IIOP), an Internet standard for CORBA communications. The IIOP communication is tunneled through HTTP to avoid customer-side firewall complications. Inprise states:

> In environments where firewalls are used to protect internal networks, communication between client applications and applets are under significant restrictions, due to the network security requirements. While these clients must be able to invoke a wide range of objects, they are prohibited from doing so by strict, and often complex, firewall configurations.
>
> There are also impediments caused by network address-translating (NAT) firewalls: This type of "so-called 'proxy firewall' creates a completely different network address -- making it impossible for a client outside the firewall to locate objects within the protected network. Rather than requiring the firewall to be configured to explicitly allow each connection from the client to server objects, VisiBroker Gatekeeper leverages its ability to proxy requests (and callbacks) through a single port on the firewall.

In addition to the Gatekeeper, we are using Visigenic's SSL Pack to set up an SSL connection between the client application and the Gatekeeper. The SSL protocol allows sensitive data to be transmitted over an insecure network, like the Internet, by providing the following important security features:

- **Authentication:** A client can determine a server's identity and be certain that the server is not an impostor. Optionally, a server can also authenticate the identity of its client applications.
- **Privacy:** Data passed between the client and server is encrypted so that if a third party intercepts their messages, it will not be able to unscramble the data.
- **Integrity:** The recipient of encrypted data will know if a third party has corrupted or modified that data.

The final piece of the security puzzle is a user digital certificate. This digital certificate is used to set up the SSL connection between the user and the Gatekeeper. In addition, the server uses the certificate to authenticate the user, in conjunction with the user's user ID and password.

Visigenic Scorecard

Requirement	**Score**	**Comments**
Security	Very good	Overall, security is very good and meets the requirements of the application
access control	Very good	Gatekeeper combined with SSL and digital certificates offers very good access control
authentication	Very good	Offers two token authentication when used with application
encryption	Very good	SSL is widely acknowledged as a good encryption standard
Traffic Control	N/A	Feature not part of the Inprise solution
bandwidth management	N/A	
server load balancing	N/A	
Enterprise Management	Good	When combined with the application, key management is adequate

key maintenance	Good	Depends heavily on application to implement
logging	N/A	Logging is done by the application
auditing	N/A	Auditing is done by the application
reporting	N/A	Reporting is done by the application
Firewall Issues	Excellent	By tunneling IIOP through HTTP, we can avoid most customer firewall issues
Timing	Very Good	Applications would likely not be delayed
Cost	Excellent	Most of the cost for this solution is already sunk; business infrastructure to support is in place
Risk	Good	Solution will meet business requirements. Most of the risk is support related
Support	Fair	Network Services has concerns about the responsiveness of the vendor

Intranet Access Analysis

It is a commonly held fallacy that an application using an intranet connection has fewer security and implementation concerns than an Internet implementation. While the risk one needs to defend against is slightly smaller if looked at one way (we're exposed only to users with access to our customers' networks), it can be much greater if looked at another way (we're to some degree trusting our customers to implement security and access control).

Any intranet-based security scheme must at minimum employ a firewall. Once a firewall is in place, allowing customer transactions to securely traverse the firewall becomes an issue. This issue is not unlike the issue of Internet access. The main difference is, on a leased line or dial up connection, there is generally seen to be little need for traffic encryption. Thus, no Secure Socket Layer (SSL) connection is required. This is the only significant advantage of an intranet solution over an Internet solution.

A word of caution regarding the security of leased lines themselves comes from UUNet, a provider of communications services including leased lines and VPNs. In a white paper entitled, **the Internet a solution to the wide area networking needs of business**, UUNet says, “Customers are often unaware that, in an FR/SMDS scenario, the only thing isolating their private network links from other customers and Internet feeds is the configuration of an FR [frame relay] switch. If the switch were compromised, or poorly configured, traffic could leak from one set of PVCs to another.” This means that even the security of a leased line can be suspect. In an intranet scenario, ACNielsen effectively delegates some responsibility for security to a third party.

In addition, there is the question of authentication. While we may allow any user in the customer’s enterprise to have access to the public side of the firewall, we need to put in place a solution to authenticate users and allow them through the firewall to bind to objects.

Intranet Security

In a white paper titled, **The Challenge: Trust in an Open, Changing Environment**, VPN vendor TradeWave states:

> Security for an intranet is based on several hardware and software components. Specific mechanisms and technology will vary, but what is sometimes called "industrial-strength" security must always satisfy the following five basic needs:
>
> - Privacy, with the ability to scramble or encrypt messages across an unsecured network
> - Access control, determining who is given access to a system or network, as well as what and how much information someone can receive
> - Authentication, which verifies the identity of the two companies executing the transaction
> - Integrity, ensuring that files or messages have not been altered in transit
> - Non-repudiation, which prevents the two companies from denying that they sent or received a file

Operating System Vulnerabilities

Internet security experts Internet Security Systems (ISS), a recognized industry leader, identifies several common areas of concern for operation systems security:

- Configuration errors. Operating system software is difficult to configure from a security perspective. A small error in configuration could result in a serious security vulnerability. File systems, for example, can be configured unsecurely, so they should be checked carefully.
- Signs of hackers. Hackers leave a trail that can be detected.
- Trojan horse programs. Hackers often implant applications in system files, thereby compromising security
- Compromised integrity of critical system files. [Check] for unauthorized modification and improper versions of critical system files. Not only does this check provide a means to detect vulnerabilities, it also helps in version control.
- Passwords. [Check] passwords against a dictionary to determine if English words are used [or] whether any passwords are related to account names or other account-associated information.

Windows NT is known to be a highly insecure operating system. Therefore, to protect the application servers, we must harden the NT boxes by following the NSA specification for securing NT servers. This specification involves a dramatic alteration to the operating system, and it is questionable whether applications will still work on a hardened box. Large sections of the NT OS must be removed or disabled to meet this specification. It is Network Services' position that this hardening must be done for any NT machine exposed in the manner proposed for an intranet solution.

Leased Line Vulnerabilities

As UUNet says, "Access control in private WANs is often a low priority where 'getting things working quickly' takes precedence over 'getting things working securely'. If any kind of access control is implemented, it tends to take one of two forms: either network-level router filters providing limited granularity of control; or simple file/drive share permissions whose underlying method of authentication is by easily-forged network address. In either case there is rarely a comprehensive audit trail kept."

According to ISS, a vendor of intrusion detection systems, "Although some organizations have well staffed and trained network security staffs, this is not the norm. The norm is a small, highly motivated, yet outgunned team that focuses most of its energies on user account maintenance, day-to-day fires, and general network design reviews. Few have time to study evolving threat, vulnerability, and safeguard (e.g., countermeasures) data, let alone develop policies and implementation plans based on the results. Even fewer have time to monitor actual network activity for signs of intrusion or system misuse."iii

Intranet Scorecard

Requirement	**Score**	**Comments**
Security	Good	Overall, security is good and meets the requirements of the application
access control	Very good	Using a firewall, we can control where users can go
authentication	Good	Without digital certificates and SSL, authentication is based on user ID and password
encryption	N/A	No encryption would be available without additional software
Traffic Control	N/A	Feature not part of intranet solution
bandwidth management	N/A	
server load balancing	N/A	
Enterprise Management	Poor	Intranet solution does not provide adequate enterprise tools
key maintenance	N/A	No keys are involved in solution
logging	Poor	Logging is done by the application and the firewall. Hard to integrate
auditing	Poor	Auditing is done by the application and at the firewall.
reporting	N/A	Reporting is done by the application; may be some reporting on firewall
Firewall Issues	Good	Firewall issues must be handled on a case by case basis with the cooperation of customer security personnel
Timing	Poor	Applications would be delayed many months; intranet solution could perhaps be put in place in 6 months
Cost	Fair	Most of the cost for this solution is in putting in place a business infrastructure to support an intranet solution
Risk	Fair	Questionable as to whether solution can provide adequate security without adding SSL, digital certificates, and a number of technologies similar to the Visigenic solution. Most of the risk is business infrastructure related
Support	Fair	Assuming the tools work and the business infrastructure is in place, the effort to support is at least 1, perhaps 2 FTEs

Virtual Private Networking Analysis

Much of the following analysis is based on a GartnerGroup Strategic Analysis Report, **Virtual Private Networking: Finding Opportunity Amid Immaturity,** dated 28 September 1998. In this report, Gartner states an important point to remember when considering VPN technology: “virtual private networking relaxes a long-held tenet of enterprise perimeter security (i.e., a general prohibition on any in-bound connections from untrusted networks), and this raises the overall level of risk that must be managed.”

Far from being a panacea for all network security and authentication problems, VPNs are seen by Gartner as a transitional technology that has tactical rather than strategic value for the enterprise. Gartner views VPNs “as a way to justify security's role in enabling new applications and ways of doing business.” Gartner cautions enterprises to “avoid the temptation to present cost shifts as cost savings.” VPNs cannot be justified on cost savings since there are so many hidden costs in their implementation.

Current and Future VPNs

Gartner states that, “In 1998 and 1999, the virtual private networking market is in its earliest stages of development: standards (e.g., IPSec) are only beginning to solidify; small start-up companies are announcing their earliest large implementations; traditional networking hardware companies (e.g., Ascend Communications and Cisco Systems) are beginning to form partnerships and make acquisitions.”

This immaturity can be evidenced in the product offerings of VPN vendors, who are just now beginning to offer their first releases of products based on the recent IPSec standard.

Gartner reports several “Strategic Planning Assumptions”, essentially predictions of the future of VPNs:

- The perception of network cost savings from remote access will drive virtual private networking growth through 2000 (0.7 probability).
- Through 2000, no one technology will successfully address enterprises' remote access, intranet and extranet virtual private networking needs (0.8 probability).
- Through 2002, virtual private networks (VPNs) on the Internet will fail to meet the reliability requirements of 75 percent of real-time intraenterprise applications (0.7 probability).
- Through 2003, less than 5 percent of all enterprises will use data VPNs to replace their wide-area networks (WANs) (0.7 probability); however, nearly 100 percent of them will use VPNs to supplement their WANs (0.8 probability).
- By 1999, virtual private networking protocol stacks will be included as part of the standard release of dominant operating systems (0.8 probability).
- Microsoft will support IPSec in at least transport mode in the server and the workstation of NT 5.0 (0.9 probability) and in future iterations of Windows 9x (0.8 probability).
- Multiprotocol tunneling standards and Internet Protocol (IP)-centric virtual private networking standards will converge by 2001 (0.8 probability).
- Creating a multivendor VPN will be almost impossible for most enterprises through 1998 (0.9 probability), which makes participation in multiple, different VPNs effectively impossible.

The Gartner report identifies several myths about VPN technology, including:

- *Virtual private networking technologies help ensure quality of service (QoS).* A VPN cannot allow an enterprise to guarantee to that a certain application will receive a set bit rate.
- *A single virtual private networking technology will meet a wide variety of implementation types.* Virtual private networking technologies make implicit assumptions about the trustworthiness of the end-user community that they support. In general, vendors tend to default to providing only basic integration with authentication and privacy through encryption.

Gartner identifies three basic drivers in virtual private networking:

- *The perception of remote-access cost savings.* The attempt to reduce remote-access costs is the number-one concern of North American enterprises evaluating virtual private networking. Through 1999, enterprises will be driven by the promise of escaping the expensive toll and leased-line charges they have incurred with the recent, continuing growth in remote access by telecommuters. Many basic Internet-based virtual private networking technologies are also extremely competitively priced and leverage Internet security investments. Very few enterprises, however, are considering the organizational costs of an Internet-based VPN, despite those costs being not subtle:

loss of manageability
variable and unassured QoS
resulting intolerance by common enterprise remote-access applications

As the realities of IP-based networking and the substantial indirect costs of using the public Internet become clearer, enterprises are expected to turn their attentions to new ways of doing business that can be enabled using virtual private networking, rather than illusive remote-access savings.

- *Increasing intranet security.* With the majority of breaches of information security coming from within the enterprise, one would logically expect significant interest in technologies that increase intranet security. In general, that has not been the case. The use of firewalls on the intranet, for example, has not become widespread because of higher expectations about transparency and performance at LAN speeds. It is also rare to see the use of strong authentication technologies (e.g., token-id cards or biometrics) because of concerns about cost, immaturity and complexity at the desktop.
- *Widening the extranet umbrella.* GartnerGroup predicts that "extranet virtual private networking" companies will be the first individual market segment to emerge from the virtual private networking market. This process will begin in 1998-99. After that, it is likely that extranet-focused companies will become effectively their own market entirely

Note that in the first driver, Gartner refers to the “perception” of cost savings. Gartner’s view is that the hidden costs of VPNs can overshadow any apparent cost savings. Enterprises should not undertake a VPN development based solely on cost. Forrester Research is a bit more positive on the question of cost. When comparing the traditional cost of Remote Access Server (RAS) versus today's Internet-based VPN, the cost differences for 1,000 users are seen by Forrester as substantial:

	Traditional RAS Costs	**VPN Costs**
Phone/ISP Charges	$1.08M	$0.54M
User Support	$0.30M	$0.00M (included in user access costs)
Capital Expenses	$0.10M	$0.02M
T1 Lines	$0.02M	$0.03M
Total	$1.50M	$0.59M

The remaining two drivers Gartner identifies are different sides of the security question, which is a key concern of the Gartner report, appearing throughout.

Types of VPNs

Gartner recommends distinguishing between data virtual private networking service providers and data virtual private networking technology providers:

- *Virtual private networking service providers* define a VPN as a WAN of permanent virtual circuits, generally using ATM or frame relay to transport IP. In this architecture, the enterprise is defined by a range of IP addresses and there are generally no additional facilities for privacy included on the network.
- *Virtual private networking technology providers* (e.g., V-ONE, Check Point Software Technologies and Aventail) define a VPN as the use of security software or hardware to bring privacy to communications over a public or untrusted data network.

Gartner also distinguishes between remote-access applications and extranet applications. According to Gartner, “Remote-access applications create an ‘extension’ to an enterprise's secure perimeter. In most cases, end users will be given the same level of trust that they appreciate when accessing from within the network, with encryption and decryption happening at or near the firewall.” Such an approach does nothing to address insider-assisted breaches of security.

“Extranet applications, by contrast,” Gartner says, “should not extend an enterprise's secure perimeter, though as a practical matter they sometimes will. From the point of view of network security, the goal of an extranet is to bring a well-defined, tightly controlled set of data to a well-authenticated third party. In contrast to the remote access case, enterprises are extremely concerned about the specific data a third-party can access on their network.” The information presented on an extranet is controlled through some sort of publishing process and security is only as good as that process.

Advantages and Disadvantage of VPNs

Virtual private networking has significant advantages over previous forms of channel encryption and alternatives, including:

- *Multiapplication support and some multiprotocol support*
- *Greater transparency to the end user after installation.*
- *No source-code modification and limited necessity for application-level integration.*

However, Gartner lists several disadvantages to VPN technology:

- *Virtual private networking technology requires client modification.* In most cases, virtual private networking vendors require that client software be installed. Client modification and deployment are easily the number-one inhibitor to virtual private networking growth. Inarguably, it is the most-often cited reason why enterprises struggle with or forestall a virtual private networking implementation.
- *The immaturity of virtual private networking technology, standards and vendors introduces unanticipated weaknesses.* In general, network security people view a new technology suspiciously and rightfully so. IPSec provides a framework for key exchange, authentication and encryption; but it does not shield an enterprise from weaknesses in particular vendors' implementations. With generally very little cryptographic expertise in the end-user community, it is undoubtedly safer to allow for a suitable period of market testing of a particular implementation of a virtual private networking standard. Weaknesses have already been seen in Microsoft's and Cisco's virtual private networking implementations and expect smaller vendors that receive less scrutiny to succumb to similar unanticipated errors in architecture or coding that will have security implications.
- *Virtual private networking technologies, even among vendors writing to the same "standards," are not interoperable.* Despite significant publicity surrounding IPSec interoperability trials in 1998, GartnerGroup estimates that true interoperability among virtual private networking vendors will not appear until the first half of 2000 (0.8 probability). All successful virtual private networking projects that GartnerGroup has seen have relied on a single vendor solution.

Gartner asserts that there are barriers to use of VPN technology, not the least of which is the lack of support within the Windows operating systems: “However, without integration with the dominant desktop operating system and with heavy reliance on young, immature start-up vendors, virtual private networking is not an appropriate technology for all remote-access, extranet and intranet applications.”

Due to the possible disadvantages of VPN technology, Gartner recommends evaluation of alternatives to VPNs.

> In single-application environments that require extreme client scalability, enterprises should consider the use of Web authorization. One alternative when deploying a legacy application to a wider-area audience is to front-end that application with a Web server, write Common Gateway Interface scripts, and use a Web-authorization technology to define the access roles and define the data set and commands that can be accessed by the end user. [. . .] The key benefit of using Secure Socket Layer (SSL) with a Web-authorization product is that Secure Sockets Layer version 2 and version 3 are widely implemented in the leading Web servers and browsers. As it requires no software distribution or support, SSL is the de facto default for Web-based consumer-to-business commerce.

It should be noted that this recommendation (except CGI scripting) describes the Visigenic security solution. This architecture uses an application proxy (Visigenic Gatekeeper) of the type recommended by Gartner.

Security, Key Management, and the VPN

Gartner stresses the importance of a “common security denominator across applications . . . including authorized, controlled access to applications at the command and file level.” This is congruent with IBM’s recommendation for security throughout the application.

Gartner is not very impressed with most current intranet security[iv]. Gartner is convinced that enterprises will move from broadcast LANs to switched LANs in the next two years, thus making VPN use in the intranet "short-lived and tactical."

In fact, all current VPN purchases need to be considered short-lived and tactical. Gartner predicts a three year lifespan, and that "the virtual private networking technologies purchased today are unlikely to be those used by enterprises in 2001; so proven capabilities in these areas - not development plans - should be central for enterprises selecting virtual private networking products." If the current version doesn't fill your needs, don't make a purchase and hope enhancements will.

Gartner recommends "any Internet-based access should also have two-factor, token-based authentication in place, the policy should also include a statement on how these tokens can be used most securely (i.e., to appreciate the real benefits of two-factor authentication for the VPN, the token should be stored separate from the laptop)." VPN vendor Check Point reinforces this point[v].

Security and Scalability Considerations

Check Point states, "Two of the three key technologies that comprise the Security component of a VPN are authentication to verify the identity of network users and data; and encryption to protect the privacy of the data. Implementing these two components will require a form of automated management to generate, distribute and control the encryption keys necessary for data privacy, and the digital signatures necessary for authentication." The third key technology is access control.

In order for a VPN to scale, careful attention must be paid to all three key security technologies as well as the question of load balancing of the application. However, management of encryption and automated access control management are the two most critical considerations for scalability.

Encryption Workload

In a VPN environment, the firewall is asked to perform significantly more work. It not only needs to be able to handle the stateful inspection tasks for increased traffic, but it also is the place where encryption and decryption of the datastream is handled. Offloading of the encryption task to specialized hardware is strongly recommended if the VPN solution is to be scaleable. Check Point, for example, partners with Chrysalis-ITS to provide boards that are plug-and-play with FireWall-1.

Access Control Management

In addition, some form of access control management must be implemented to manage lists of authorized users and their encryption keys. Entrust Technologies and Check Point are partnering to provide unified enterprise security solutions that include firewalls, VPNs and remote access with a single public-key infrastructure (PKI) for automated key management that is IPSec-compliant. Their product will be released by the end of the year.

Finally, authentication should be handled using a strong, two-factor token-based scheme and the industry-standard RADIUS (Remote Authentication Dial-in User Service) protocol.

Gartner cautions that:

> "Extranets are the proving grounds of technical and organizational skill in information security, and should be used by enterprises with proven expertise in information and network security[vi]. Perhaps no other networking application spans as many of the information-security market segments - from authentication to management and consulting - as the opening up of trusted local resources to an enterprise's business partners or customers. Virtual private networking technologies that provide LAN-to-LAN-encrypted or LAN-to-PC-encrypted IP tunneling are generally insufficient for this task. The key is using a VPN that provides granular access control, up to full application proxies, in combination with Web-authorization tools and strong, token-based authentication. An early problem arises in that the vendors that focus the most energy on value-added services necessary for the extranet are also the most proprietary in implementation."

VPN Implementation Issues

Gartner states, "Networking issues, even more than security questions, create some of the greatest areas of complexity for enterprises implementing VPNs. The dominant virtual private networking interoperability standard, IPSec, was designed to meet the needs of large networks with large amounts of unique IP addresses. Thus, IPSec makes little accommodation for handling the complexities of NAT and DNS."

A major stumbling block in the implementation of a software-based VPN solution is Network Address Translation (NAT). This refers to the technique of masking the true IP address of a client behind a firewall, and substituting a common IP address for each user. For example, all users from ACNielsen appear to hosts on the Internet to be coming from 206.102.161.11. Software-based VPN schemes rely on knowing the true IP address of the client.

Gartner is also concerned with the coexistence of VPN clients on the client PC. If our clients are also implementing VPN technology, but using different vendors, there could be "significant volatility on clients where multiple virtual private networking technologies are installed."

VPN Implementation Recommendations

Gartner suggests enterprises first execute a pilot implementation before fully adopting a VPN solution. The steps in the pilot include:

- Security Audit
- Define the Scope and Application Needs (including Quality of Service issues)
- Documentation (a statement of understanding for the extranet VPN partners)

Gartner recommends the following criteria in evaluating VPN networking vendors:

- Network Performance (latency and packet loss)
- Pricing (Most data VPNs cost about 5 percent to 10 percent more than Internet access with the same bandwidth
- Geographic Coverage
- Data Integration
- Deciding on the Underlying Network (Enterprises are advised to build their intraenterprise VPNs on private IP networks, not the Internet)

Gartner recommends the following criteria in evaluating VPN software vendors:

- *Scalability* (per-seat price, growth of the application, processor burden of cryptography, load-balancing, redundancy, facilities for monitoring performance and packet loss)
- *Security* (integration with authentication and access control, appropriate granularity of control and extent of privacy, support or require the use of X.509 certificates, support strong authentication)
- *Manageability* (monitor, manage and trouble-shoot, flexible configuration, remote and hierarchical management, auditing and monitoring)
- *Simplicity* (Are the administrators shielded from the complexity of the underlying encryption algorithms? How complicated is the installation on the client?)
- *QoS* (Can the virtual private networking technology set priority by traffic type? Can it allocate bandwidth dynamically to simplify load-balancing?)

ACNielsen VPN Implementation

Gartner says, "In this early stage of market development, the virtual private networking technology market has no leaders and no clear segmentation." They feel the entrance of traditional networking companies could crowd out the pure VPN players (e.g., Aventail and Kyberpass). "Chief among these is Check Point, with 43 percent of the global firewall market and an early, if until recently undermarketed, virtual private networking product. [. . .] Cisco has also traditionally suffered from a lack of focus in the network security market, as evidenced by a large, but generally disparate, security product line. [. . .] Microsoft warrants inclusion because of its hold on a crucial piece of the virtual private networking architecture: the integration of a virtual private networking client at the desktop."

For an ACNielsen solution, two vendors were analyzed as potential providers of a VPN solution:

- Microsoft's Point to Point Tunneling Protocol, as provided in Windows NT 4.0 and various Microsoft products
- Check Point VPN-1 family of products

Protocol Tunneling – Microsoft and Cisco

Protocol tunneling, of which a good example is Point to Point Tunneling Protocol (PPTP), is one of the two major classes of technology used in virtual private networking. According to NT Systems' white paper[vii] on VPNs, written by the president of VPN vendor Aventail:

> Current VPN architectures are based on two models: the directed VPN or the tunneled VPN. Directed VPNs function at the session layer (layer 5) of the OSI network hierarchy. Directed VPNs offer unidirectional connections between corporate sites so the data exchange is highly controlled and monitored. A two-way trusted relationship is not assumed like it is with tunneled VPNs. Tunneling creates LAN-to-LAN or client-to-LAN connections at the packet level based solely on source and destination. Also, if security is breached in the directed model, only the destination network is affected. In the tunneled model, the connections expose both the source and destination networks, so companies are more likely to inherit the security flaws of their VPN partners. In general, the higher a VPN is implemented in the OSI network model, the more secure it is because fewer changes are required to the network infrastructure. The tradeoff is performance, which is better at the lower layers.

Microsoft and Cisco are leaders in the PPTP arena, along with the PPTP Forum members Ascend Communications, 3Com/Primary Access, ECI/Telematics, and US Robotics.

Gartner states, "Microsoft and Cisco have been criticized by independent third-party cryptographers for weaknesses in their implementations, presaging what is likely to be more general criticism of the large traditional vendors as they build skills in cryptography, focus resources and receive their first feedback from large enterprises." Microsoft has integrated PPTP technology with its RAS solution, which supports bulk data encryption using RSA RC4 and a 40 bit session key negotiated at PPP connect time between the RAS client and the Windows NT RAS server. It should be noted that 40 bit encryption is not considered industrial-strength, although it does meet the US Government's restrictions on encryption exports.

In another context, Gartner says:

> Microsoft has given mixed messages on its support of emerging standards in the virtual private networking market. Although clearly supporting PPTP publicly, it made a number of early implementation errors at the client and the server that, while later largely patched, further confirmed that network security remains a low priority for the company. Its support for IPSec was not solid until well into 1998 when the larger part of the vendor community had roughly coalesced around the standard. This created a vacuum at the desktop for most of the early virtual private networking start-up companies that chose to bundle their own client rather than wait for Microsoft to move decisively. Small vendors distributed their own IPSec-compatible clients, often deploying as an NDIS shim to the TCP/IP stack. These IPSec shims are an ad hoc solution at best, even in the eyes of the vendors that developed them, as they are difficult to deploy and install and are the frequent cause of technical support calls. No leading start-up vendors have built their business plans on the long-term sales of these or any proprietary client.

This means that the use of Check Point's SecuRemote or other vendor's IPSec shim is likely to be a short term solution, until Microsoft asserts a de facto standard by integrating VPN support into their operating systems. Gartner recommends that, "Enterprises should consider virtual private networking client-software purchases as tactical decisions and negotiate vendor contracts accordingly."

Microsoft's VPN solution is based on PPTP, has had numerous security problems, is basically a type of packet filtering (see previous), and is only supported on WinTel hardware. It is similar to a related protocol, Layer Two Transport Protocol (L2TP). In a white paper entitled **Making Sense of Virtual Private Networks,**[viii] VPN vendor Aventail delineates the strengths and weaknesses of these protocols:

Advantages

- ready-made to work with the latest versions of Microsoft systems
- typically less complicated to implement because they use packet-filtering with existing network routers
- transparent to end users
- PPTP is free
- support additional networking protocols such as Novell's IPX, NetBEUI, and AppleTalk
- support flow control
- enhance network performance by minimizing dropped packets

Disadvantages

- tunneled approach to VPN security: encapsulate non-secure IP packets within secure IP packets, create an open data passageway between two computer systems
- once tunnel is open, source and destination identification no longer required
- tunnel is bi-directional, and does not provide a way to monitor or control what gets passed between the two points
- limited to 255 concurrent connections
- end users are required to manually establish a tunnel prior to connecting to the intended resource
- selection of authentication and encryption standards is very limited, and currently no strong encryption or authentication is supported
- no versions of PPTP or L2TP available for older Microsoft operating systems or UNIX
- PPTP and L2TP are currently only proposed standards

In addition, as Microsoft states, “Because PPTP requires RAS and the PPP protocol, you must establish a PPP account with your ISP to use PPTP over an ISP connection to the Internet.”

Simply put, PPTP is not a VPN, a point of view shared by router and PPTP vendor Ascend, who states: “The VPN is the application, while PPTP is the protocol used.” It offers the enterprise very little control over what flows into and out of the network, and offers limited authentication choices. In addition, it is Network Services policy that Windows NT machines will not be exposed to the Internet, due to inherent weaknesses in security of that OS. Although Microsoft says a PPTP server can be placed behind a firewall, the firewall would not be able to do stateful inspection on the PPTP traffic, and thus only provides a small amount of extra security. Therefore, Microsoft’s PPTP technology is not an option for ACNielsen.

Microsoft PPTP Scorecard

Requirement	**Score**	**Comments**
Security	Poor	Overall, security is unacceptable due to vulnerabilities in Windows NT
access control	Poor	Access control is based on Windows NT, which is easily compromised
authentication	Poor	Normal Windows NT procedures are used
encryption	Fair	PPTP standard is good; Microsoft's implementation has had problems, and is limited to 40 bit keys
Traffic Control	N/A	No traffic control is available in this solution
bandwidth management	N/A	
server load balancing	N/A	
Enterprise Management	Poor	Management tools are essentially Windows NT-based
key maintenance	Poor	No ability to rotate keys
logging	Poor	All access is logged within Windows NT Event Log
auditing	N/A	No auditing is possible, outside the Windows NT Event Log
reporting	Poor	No integrated reporting is available
Firewall Issues	Fair	Customer firewall and ISP must be configured to permit PPTP traffic
Timing	Fair	Applications would be delayed many weeks; PPTP solution could perhaps be put in place in 2 months
Cost	Excellent	Software is essentially free; most of the cost for this solution is in putting in place a business infrastructure to support
Risk	Poor	Poor track record of Microsoft regarding security solutions; inadequacy of solution to fulfill business requirements
Support	Poor	Restricted to typical Windows NT administration tools, which lack scope; the effort to support is at least 2, perhaps 3 FTEs

IPSec Tunneling – Check Point

Our current firewall, FireWall-1 from Check Point, is ready to implement a software, or client, VPN solution. A piece of software called SecuRemote is installed on the client's Windows 95 or NT PC and provides encryption of the datastream. When the user attempts to connect to ACNielsen services, the SecuRemote software pops up a dialog for credentials, which can be part of the user authentication and access control solution. However, there's work to do on the back end to enable this and an owner for the maintenance process on an ongoing basis needs to be identified.

SecuRemote is IPSec based and is very secure. The problem is that for versions up to SecuRemote 3.0b (our current version), users behind a Network Address Translation (NAT) gated firewall (like ours) cannot be supported due to the NAT. It is thought that all or most of our clients use NAT technology. The SecuRemote 4.0 client has just been released, and NAT support may have been included.

Gartner's warning about possible incompatibilities between any VPN client software we would use, and VPN client software that a customer may implement for their own purposes is a definite risk.

VPN Authentication

We would use the Entrust model, which provides for one certificate of authority for all VPNs (VPN-1 Certificate Manager). This software is available from Check Point in December, 1998. Unfortunately, this is a brand new technology, and would require lots of research to implement.

We would use Cisco's RADIUS implementation as the authentication solution for user accounts. Standardization on a single authentication method and vendor would have implications to other systems currently in place. For example, currently dialup is handled by a Cisco secure box using TacX for authentication. This solution would not scale to the enterprise, and thus we would need to change to RADIUS. Doing so would leverage the existing dial up security database across all applications.

Enterprise Management

It cannot be stressed too strongly that there are considerable administrative and operational issues surrounding the maintenance of security and user keys. Key management is not a trivial task, and this needs to be understood across the enterprise.

Check Point has a newly-released product called Provider-1 which, although it is primarily targeted at ISPs, has industrial strength management capabilities that would be of great use to ACNielsen. Features include:

- Merge multiple FireWall-1 Management Consoles to a single hardware server
- Offer a consolidated view into the entire customer base
- Isolate customer databases
- Segment customer databases into manageable sizes
- Allow customers to manage their own user databases
- Simplify operations
- Provide a single point of backup
- Scale to hundreds of customers with thousands of enforcement points
- Distribute logging and alerts

Check Point enables the installation of up to 50 FireWall-1/VPN-1 Management Consoles on a single hardware server. This means that ACNielsen can administer up to 50 different VPNs on one box and service multiple applications as separate virtual networks. In addition, hardware servers can easily be added as managed services grow, keeping initial and incremental investment costs low.

Provider-1 offers an easy-to-use GUI for management, monitoring status and alert information of the entire customer base. Using FireWall-1/VPN-1's security policy editor, many administrators can concurrently manage multiple customers' security policies, using encrypted communications. MSPs can also delegate selected management functions (e.g. user management) to customer sites while retaining control over other core management functions (e.g. security policy management).

Provider-1 utilizes a FireWall-1/VPN-1 mechanism that allows logs and alerts to be redirected to many different destinations, either in real-time or on a predefined schedule. This Customer Log Module (CLM) allows customers to have on-line access to their own logs.

This is a new product from Check Point, and therefore, there is an attendant risk. However, if the product performs as advertised, it represents a complete enterprise administration solution for VPNs. Pricing is not yet available.

OS Vulnerabilities

According to UUNet, "Encryption of data passing between systems on the WAN only protects information being transmitted; it does nothing to secure the operating systems and application generating the traffic. The ability to scramble confidential information in transit is of no consequence if an attacker can easily gain access to the end systems and monitor the data before it is sent. For this reason it is vital that privacy and access-control are used in tandem." This means that any operating system and operating hardware exposed to the public needs to be assessed for risk.

An alternative to a client VPN is a firewall to firewall or firewall to router VPN. These are dedicated VPN connections between two hardened boxes, one on the customer site, and one at ACNielsen. This represents a permanent secure circuit that's always there. However, this solution costs significantly more due to the dedicated hardware. It is not possible to leverage existing equipment at client site; new equipment must be put in place and dedicated to the VPN. In addition, this solution is likely to meet with lots of resistance from the customer's datacom group. This is because we can't give encryption keys to remote client staff, and need to administer the VPN equipment remotely ourselves.

As a side issue, it would be possible to replace existing customer leased lines with an Internet VPN. While this might cut costs, we would face significant QoS issues, and client policy issues. Policy issues on both the ACNielsen and customer side would make implementation slow.

Check Point Scorecard

Requirement	Score	Comments
Security	Excellent	Overall, security is excellent and meets the requirements of the application
access control	Excellent	Using a firewall-based VPN, we can control where users can go
authentication	Excellent	Two token authentication provided by VPN
encryption	Excellent	Ability to rotate keys periodically
Traffic Control	Good	Check Point's traffic control software is new, and it's hard to evaluate
bandwidth management	Good	Allows administrator to assign bandwidth to applications
server load balancing	Good	Check Point has a load balancing scheme
Enterprise Management	Excellent	Check Point partners with other vendors to provide a complete solution
key maintenance	Excellent	Check Point's management solution is based on a third party vendor
logging	Excellent	All access is logged and logs are accessible within management console
auditing	Excellent	Real time auditing is possible
reporting	Good	Integrated reporting is available
Firewall Issues	Good	Firewall issues probably isolated to ACNielsen side and are solved with hardware: accommodating encryption load and increased bandwidth demands. Customer NAT firewalls may be an issue.
Timing	Poor	Applications would be delayed many months; VPN solution could perhaps be put in place in 6 months
Cost	Fair	Most of the cost for this solution is in putting in place a business infrastructure to support a VPN
Risk	Fair	Lots of new technology in its first revision would need to be implemented. Most of the risk is business infrastructure related
Support	Good	Assuming the tools work and the business infrastructure is in place, the effort to support is at least 1, perhaps 2 FTEs

Endnotes

[i] White paper published as part of Whire newsletter, October, 1998, http://www.whittmanhart.com/pdfs/minnoct98.pdf.

[ii] According to class materials from the University of Colorado, **Firewalls: What They Are And How They Work** (http://www.colorado.edu/infs/jcb/sinewave/network/firewalls/applic.html), "The application gateway, or proxy as they can be referred to, operates at the application level. The proxy resides on the gateway computer (similar to the relay in the circuit gateway). A proxy works very similar to a circuit gateway except that the proxy is written for a specific application such as HTTP or FTP. If the network traffic is not of the same format as the proxy, it is not permitted past the gateway. Another difference between the proxy and the circuit gateway is that the proxy understands what it is filtering. The reason that this is possible is that the proxy incorporates some of the applications protocol so that it speaks the same language as the application. This allows the proxy to selectively filter according to type of request, for example. With this being so the proxy is no longer totally transparent to the user. The user may need to redirect the connection request to the application gateway or a different set of commands than is usually required to connect to the other side of the firewall."

iii In the white paper, Getting Past The Cyberspace Hype: Adaptive Security, ISS states: "The following outlines the typical sequence of events within organizations implementing [a typical security] approach:

1. Organizational managers tend [to] See the Network, but not in the context of the actual risk conditions. They understand the basic technology differences between operating systems such as Windows NT and Sun Solaris. They also understand how products such as Netscape, Internet Explorer, Word, Powerpoint, and Excel enhance their operations. But, they have little knowledge about the associated vulnerabilities that allow threats to enter, steal, destroy, or modify their most sensitive data.

2. [. . .] safeguards are implemented in an ad-hoc manner. This is largely due to an incomplete understanding of the problem. There is no real traceability to operational requirements, no study of the effects on threats or vulnerabilities, and no analysis of the return on investment. This approach can be summarized in the formula: SECURITY = DIRECT TECHNICAL COUNTERMEASURES (i.e., firewalls, encryption, security patches, etc.).
3. [. .] organizations applying safeguards in this manner are left with a false sense of security. They believe they have addressed their risk, when in fact, many threats and vulnerabilities have not been taken into account. Considering the results of the various studies, it appears this approach provides an overall 20-30% solution.
4. Over a relatively short period of time, the risk conditions further degrade. This network security degradation occurs as users alter system and safeguard configurations and work around safeguards.

[iv] Gartner says most intranet security depends on "department-level privacy and transparency. [. . .] In some cases, these networks become 'accidental extranets' where all the data and resources of independent subsidiaries, contractors and outsourcers can be accessed on the same shared private network, eroding the concept of the trusted network."

[v] In *Redefining the Virtual Private Network*, Check Point says, "And as one considers the user authentication schemes offered, it is important that a strong two-factor authentication scheme is available as an integrated option. Strong two-factor authentication schemes provide maximum security over the more traditional username/password system because it requires two elements to verify a user's identity (usually an electronic token and a PIN number). In this manner, the user must have something in his possession and something he memorizes. This drastically reduces the probability of someone impersonating a user because he needs both elements to access the system."

[vi] Gartner feels that, "Enterprises should define 'policy control points' in the network where firewalls, intrusion detection and virtual private networking can most effectively and safely monitor and segment the network."

[vii] NT Systems' white paper can be found at http://www.ntsystems.com/nts107fe.htm. It has this to say about Microsoft's PPTP solution: "With the introduction of NT 4.0, Microsoft introduced PPTP as its solution to VPN demand. It sits at the data-link layer, so it is limited to packet filtering for access control. Packet filtering is generally less secure than the proxying method deployed by most firewalls. PPTP cannot filter data by the type of application, the content of the application, or the authentication or encryption method used. PPTP's big advantage is that it can handle IPX and IP traffic. This is critical for network administrators who want users to use IPX-based services remotely."

[viii] In a white paper entitled **Making Sense of Virtual Private Networks** (http://www.aventail.com/index.phtml/solutions/white_papers/vpnmarketwp.phtml), VPN vendor Aventail describes the PPTP and L2TP protocols:

"One of the most widely known VPN security choices is Point-to-Point Tunneling Protocol (PPTP) from Microsoft. It is embedded in Microsoft's Windows NT v4.0 operating system and is used with Microsoft's Routing and Remote Access Service. It sits at the datalink layer, which maps approximately to layer two of the OSI model. It encapsulates PPP with IP packets and uses simple packet filters and the Microsoft Domain networking controls to provide access control. PPTP and its successor, L2TP, are seen as tools to extend the current PPP dial-up infrastructure supported by Microsoft, most ISPs, and the remote access hardware vendors.

"Layer Two Transport Protocol (L2TP) has evolved from the combination of Microsoft's PPTP protocol and Cisco Systems' Layer 2 Forwarding (L2F). It supports multiple, simultaneous tunnels for a single client and is targeted at the telco and ISP markets. With L2TP, the end user dials up a local ISP POP without encryption, and the ISP, acting as an agent for the end user, creates an encrypted tunnel back into the secure destination.

"PPTP and L2TP have received broad support from the current leaders in the remote access services market, which includes Cisco, Bay Networks, 3Com, Shiva, and Microsoft, because they provide an effective way for these vendors to migrate their current corporate dial-up products to Internet-based methods of building tunnels. Analysts predict that PPTP and L2TP will play a dominant role in the Internet-based remote access market when security requirements are relatively low.

Advantages

“IS professionals running Microsoft-centric shops will find PPTP and L2TP ready-made to work with their systems. Because they use packet-filtering that makes use of existing network routers, they are typically less complicated to implement, and they are transparent to end users.

“In typical Microsoft fashion, PPTP is free. Microsoft includes it as a component of its RAS and router software, formerly known as Steelhead. When affordability in a Microsoft-only environment is an issue, PPTP is a viable solution. L2TP will likely follow the same path and be included in upcoming versions of NT servers and Windows 32-bit desktop clients.

“Most VPNs secure TCP/IP traffic, but PPTP and L2TP support additional networking protocols such as Novell's IPX, NetBEUI, and AppleTalk. They also support flow control, which keeps traffic from overwhelming clients and servers. They enhance network performance by minimizing dropped packets, thus cutting down on re-transmission.

Disadvantages

“PPTP and L2TP are typical tunneled approaches to VPN security, which means they encapsulate non-secure IP packets within secure IP packets. They use IP frames to create an open data passageway between two computer systems. Once a tunnel is open, source and destination identification is no longer required. The tunnel is bi-directional, so while it encrypts data traveling along the Internet, it does not provide a way to monitor or control what gets passed between the two points.

“One often overlooked limitation is that PPTP and L2TP are limited to 255 concurrent connections. In addition, end users are required to manually establish a tunnel prior to connecting to the intended resource, which can be a hassle. Also, the selection of authentication and encryption standards is very limited, and currently no strong encryption or authentication is supported.

“Another concern is that there are currently no versions of PPTP or L2TP available for older Microsoft operating systems or UNIX. PPTP is still very narrowly targeted for Microsoft-specific networking.

“PPTP and L2TP are currently only proposed standards. PPTP is presently supported by Microsoft's Windows NT 4.0 server, NT workstation, and Windows 95. Remote access vendors, such as Ascend and Shiva, are backing L2TP, and Microsoft plans to incorporate L2TP into Windows NT server version 5.0.”