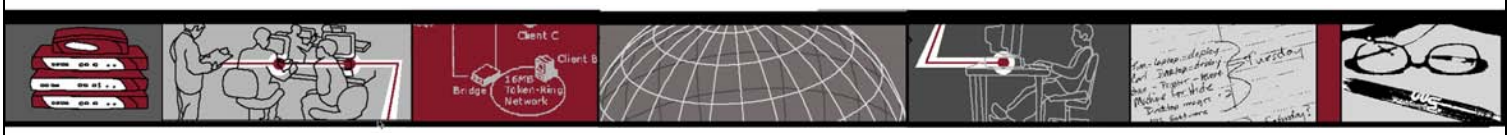

STRAIGHT TALK ABOUT VPN

IT'S NOT MAGIC, BUT IT IS THE ANSWER

JULY 2002

WatchGuard Technologies
505 Fifth Avenue South
Suite 500
Seattle, WA 98104
www.watchguard.com

STRAIGHT TALK ABOUT VPN

IT'S NOT MAGIC, BUT IT IS THE ANSWER

You're waiting to cross a crowded downtown street at night, when a long black limousine zooms past. Its darkened windows reflect neon signs, giving away nothing about who is inside or what they're doing. You can't help wondering what that sleek exterior hides: Diplomat? Crime boss? Movie star? The light changes, and the limo vanishes into the night, leaving behind nothing but your speculations.

Translate that experience into the world of the Internet, and you can grasp what's cool about VPNs (Virtual Private Networks). Just as the limousine drives the public streets but keeps its contents private, a message sent via VPN travels the public Internet, but is encapsulated in encryption so that its content remains private. Only the originator and the receiver of the message see it in a clearly readable state. Any hacker trying to eavesdrop en route gets nothing but a scrambled mess. The path of a VPN message has "light" at each end but "darkness" (obscurity) at all the between-points, so it is called, metaphorically, a VPN tunnel.

Where private business communications were once the privilege of the largest corporations, who could afford their own private networks, now VPN technology allows almost anyone with a computer and access to the Internet to send and receive data confidentially. VPNs are rapidly moving from merely being a trendy phrase, to being essential for wired business.

How is a VPN used? Is it right for every business? What should businesses watch out for when implementing VPN technology? Answers ahead.

TYPICAL VPN SCENARIOS

While there is no such thing as a "typical" VPN configuration, there are some business scenarios where VPN technology brings outstanding benefit. VPNs are usually used for:

- Mobile users
- Branch offices
- Extranets

We'll consider each one individually.

MOBILE USERS

Whether we're talking about telecommuters who work from home, or road warriors who want access to the corporate network from constantly changing locations, Mobile User VPN (MUVPN) enables connections from remote computers to the corporate network, while maintaining privacy and security.

Sharp network administrators worry about two security problems related to mobile users:

1. Someone tapping the exchange of information between the remote user and the network; and

2. Someone depositing malicious code on the remote user's computer while it's connected to the Internet from outside the company firewall - code that the remote user later brings back into the company with them.

MUVPN solves the first problem by encrypting sessions, so that no eavesdropper can intercept plain-text messages.

The second problem is both more likely to happen, and tougher to solve. When a sales representative uses the Internet from a hotel, any worm or bug might crawl onto her laptop. When she returns to headquarters, carries that laptop to the docking station at her desk, and logs into the corporate network, she's just carried whatever is on her computer past the firewall. To prevent this, any MUVPN solution should also be integrated with anti-virus software and a personal firewall on the laptop - that way, the device that is accessing the corporate network from outside is less susceptible to attack.

BRANCH OFFICES

In this scenario, geographically separated offices within a corporation need to pass data to one another, or to access a common database. For example, in a retail chain each location may need to check inventory in the same centrally located warehouse.

Branch office communications involve sensitive security issues because these locations often send and receive the kind of critical, intimate data exchanged between users inside corporate headquarters. VPN enables confidential connections from site to site.

WatchGuard's VPN Manager uses proprietary DVCP™ technology to simplify the creation of VPN tunnels by identifying the necessary configuration settings for a network of Fireboxes® and automatically establishing IPSec VPN tunnels between locations. This automated setup drastically reduces the complexity of the task. Using VPN Manager, network administrators can centrally manage and monitor VPN traffic from anywhere in the world.

WatchGuard's Firebox System supports extranet deployment by allowing you to establish restrictive security policies on individual tunnels with business partners. That way, the access available via those tunnels to servers, services, and networks can be limited to the minimum necessary to achieve your goals. Some competing devices offer "all or nothing" extranet access. They can't apply nuanced security policies to VPN tunnels the way WatchGuard products can.

From a network administrator's viewpoint, branch offices present another challenge: typically, when the network administrator tries to set up a VPN tunnel to a branch office, there's no one on the other end qualified to help him.

The traditional solution: the network administrator travels all over the globe fixing the tough problems at each location. The modern solution: businesses can choose VPN solutions that include remote diagnosis tools and location-independent management capabilities. Ideally, the network administrator should be able to manage all VPNs from any location. This eliminates the expenses of traveling to the branch offices, or of requiring technically advanced personnel at the other end of each VPN tunnel.

EXTRANETS

Using VPN technology, separate business entities who work closely as partners (e.g., a raw materials supplier and a manufacturer; a medical lab and a hospital) can safely and efficiently share information about their mutual business, without having to give each other access to the rest of their networks. These extranet installations resemble branch office implementations, but use vastly more restrictive rules for sharing data. These rule sets are imperative for secure extranet implementation, since each party is opening part of its network to outsiders.

Hardware compatibility presents the biggest obstacle to extranet VPN implementations. To ensure flawless compatibility, large companies usually standardize on one brand of firewall, one brand of router, one brand of switches, and so on. When two independent businesses work together, they usually have each standardized on different gear, and neither party can dictate to the other what equipment to use. The issue of establishing a VPN while using equipment from multiple manufacturers and vendors is referred to as interoperability, which is discussed further in the next section.

Now you've had a whirlwind tour of the most common VPN uses. But implementing a VPN is not a trivial task. To learn about some of the technological challenges of causing a VPN to run smoothly, read the next section.

The WatchGuard Firebox line has models priced to fit all budget categories. Each device comes with a renewable subscription to LiveSecurity® Service, which provides ongoing education and technical support to the user and software updates to the Firebox so that your defenses remain up-to-date.

VPN Manager automates the process of creating tunnels and simplifies it to a drag and drop operation, in some cases reducing the 45 minute setup time to mere seconds.

FINE, BUT WHAT'S IT REALLY LIKE?

While VPN solves many problems for geographically distributed enterprises, it doesn't do so magically. Implementing VPN implies a level of ongoing commitment -- it's not a set-it-and-forget-it answer. There are a few sticking points to VPN, which require forethought to overcome. The most common problem areas are:

- Interoperability
- Scalability
- Management and Total Cost of Ownership

This next section suggests solutions to each of these problem areas.

INTEROPERABILITY

To address the issue of interoperability, standards organizations have developed a worldwide criterion called IPSec (Internet Protocol Security). IPSec defines the rules by which devices from any number of vendors can work effectively together. IPSec is better than anything that came before it, but is neither perfect nor simple. Many vendors implement IPSec with slight differences.

The International Computer Security Association (ICSA *www.icsalabs.net*) has stepped in to provide an objective evaluation about which vendors truly comply with IPSec standards. ICSA-certified products are guaranteed to interoperate. So, in selecting a VPN solution, businesses should seek ICSA IPSec-certified products to avoid getting stuck with technology that is not compatible with the rest of the world, forcing major purchases later.

Many security vendors, including WatchGuard, Cisco®, Check Point™, Nokia®, and others, maintain a public list of other vendor's equipment with which they operate, and instructions on how to get VPN working. For the prospective buyer, this is an easy issue to research.

SCALABILITY

If a business grows, it needs more equipment. That's why there's a new IT budget every year. Businesses about to buy VPN solutions should think about today's needs and what they'll need if the next two or three years go well. Some VPN solutions fail once you have five or six sites. The best VPN technology has scalability, the ability to grow in scope without exorbitant expense or labor.

Attributes of a highly scalable network include:

- Additional components are affordable
- The system is designed so administrators can readily manage many or few components
- Devices are available in many different price and performance ranges
- Diverse devices can be managed from one application anywhere there is a network connection

In addition to Industry- leading ease of use, WatchGuard's Fireboxes come with outstanding technical support. WatchGuard's standard support is similar to some of our competitor's premium support. WatchGuard's Gold Support targets a one-hour response time to customers, around the clock, around the world.

MANAGEABILITY/TOTAL COST OF OWNERSHIP

To an organization that has no VPNs, the idea of super-secret data tunnels can seem like a luxury at first. Businesses often assume they'll only need a few VPN tunnels. But any business that distributes sensitive data - and especially, any business that has experienced an embarrassing or costly security leak - quickly falls in love with the strong privacy of VPNs. VPN technology then gets applied to more and more of the business's communications. Even small to mid-size business may use 100 tunnels, and networks using many times that number of tunnels are common.

This heightens the importance of good management technology for your VPN. Assuming qualified operators on both ends and a good telephone connection, setting up a normal VPN tunnel can take 45 minutes. If you need merely one tunnel, 45 minutes is not a big deal; people waste that much time on coffee breaks. But for a larger corporation, multiply 45 times 100 tunnels, and suddenly the amount of time necessary to set up, change, and maintain a VPN becomes a major factor in selecting a VPN product.

Money saved on a VPN that has a low initial cost can turn into money lost if that VPN is time-consuming to manage and confusing to maintain. Plus, solutions that are simple to use are more likely to be used correctly.

The ideal solution will have a simplified management interface; the ability to aggregate logs from numerous sources, and advanced features that work in multimode networks.

TAKING THE PLUNGE

The best advice for a corporation ready to deploy its first VPN is this: spend a lot of time doing your homework. (To help you get started, we've provided a Firebox comparison at the end of the document.) It's easier and more efficient to study up on all the issues that surround a specific implementation, than it is to fix a misguided VPN installation after it's set

up. The first step is to find a trusted resource of expertise who can help you figure out your issues - then, pay attention to his or her advice. Start slowly. Begin with a small deployment to see if it really meets your needs, before you deploy widely.

Though VPNs require some time and attention, as the standards are becoming more mature, more people are using VPN technology. Vendors have made tremendous improvements in usability, reporting, logging, and management. Other barriers to entry, such as price and complexity, are coming down. Now, any organization that is still transmitting confidential data in the clear as e-mail attachments, or buying privacy through expensive leased lines, should consider implementing a VPN.

After all, if you lose your company secrets to a competitor - how will you ever get to ride in that limousine?

THE WATCHGUARD PRODUCT LINE

The WatchGuard Firewall line is divided into two families, the Firebox III / Firebox SOHO family, and the Firebox® Vclass family. Each family is optimized for the needs of a particular class of business. For organizations that place a high priority on VPN throughput, flexible management options, and advanced network management features, we offer the Firebox Vclass line of products. For smaller organizations that place a high priority on ease of management and a full feature set, we offer the Firebox III / Firebox SOHO family.

As the table indicates, a smaller remote office or business will find enough horsepower in the Firebox 700. If VPN tunnels are a factor in your plans, you'll want to look closely at the Firebox 1000 for those same offices. If the office is a little bigger, check out the numbers for the Firebox V60. If you have 1000 to 5000 users and use the Web heavily, or run a mid-size business, we recommend the Firebox 2500. If you're firewalling a larger enterprise in the 1000 to 5000 user range, and have heavy VPN needs - well, we think the Firebox 4500 or V80 is just what you're looking for. For gigabit VPN and carrier grade network management choose the Firebox V100.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

E-MAIL:
information@watchguard.com

U.S. SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.521.8340

FAX:
+1.206.521.8342

ABOUT WATCHGUARD

WatchGuard (Nasdaq: WGRD) is a leading provider of dynamic, comprehensive Internet security solutions designed to protect enterprises that use the Internet for e-commerce and secure communications. Thousands of enterprises worldwide use WatchGuard's award-winning products and services. These products include our Firebox firewall and VPN appliances for access control and secure communications, and our ServerLock technology and anti-virus solution for content and application security for servers and desktops. Centralized point-and-click management makes it easy for even the non-security professional to install, configure, and monitor our security solutions. Our innovative LiveSecurity Service also enables our customers, with minimal effort, to keep their security systems up-to-date in a continuously changing environment. For more information, please call 206-521-8340 or visit *www.watchguard.com*.


Client C
Client B