How Firewalls and Secure Virtual Private Network Hardware Can Be Combined for Robust Corporate Security

By Cary Hayward
Product Marketing Manager
RedCreek Communications, Inc.

The Current Environment

Increasing use of remote access, along with the demand for faster and lower-cost connectivity, has contributed to Corporate America's interest in public data networks, such as the Internet, for day-to-day data communications. The remote access market is taking off rapidly. Total revenues for this market are expected to surge by 75%, to $4.5 billion in 1997, according to International Data Corp., a research firm in Framingham, Mass.[1] A good part of the reason for this is that an Internet-based approach is estimated to save up to 60% by using public networks (e.g., Internet) over equivalent private (e.g., leased line) networks, according to a 1996 Forrester Research study.[2]

What are the hurdles that need to be cleared before the Internet really takes off? Many corporate network managers remain concerned about the reliability and security of the Internet. These concerns are valid. Corporations want reliable bandwidth public data networks, and historically leased-lines have been the standard solution. This is starting to change as the carriers and Internet Service Providers(ISPs) move aggressively to address Internet reliability issues. Some providers are so confident that they can deliver reliable Internet connectivity, they are guaranteeing throughput with a money back guarantee. One ISP is offering a service-level satisfaction of 99.5% backbone-access availability with delays of less than 70 microseconds in the continental U.S. Carriers and ISPs are promoting virtual private networking services as augmentations to leased lines and frame relay or even as the turnkey solution for interconnecting corporate local-area networks (LANs).

Well-publicized cases of break-ins by network hackers have scared corporations. A 1997 survey commissioned by the FBI and Computer Security Institute found that in 1996, 75% of 563 survey respondents suffered known financial losses due to security breaches. Ninety-five percent of all software/data theft goes undetected by the corporation. In 1996 financial fraud totaled $24.9 million, and theft of proprietary information had an estimated cost

of $21 million.[3] This data is the driving force behind the growth of firewalls.

As companies use public and private networks for communication between their geographically dispersed offices, there is concern with maintaining the security of the information. Why? It is easy and inexpensive to stage "man-in-the-middle" attacks where data passing over a public or private network is grabbed (capturing information going over the network is called "sniffing"). Software that can be used for this purpose is commercially available for around $100 and runs on any laptop. An intruder can connect the sniffer to any switch, hub, or router on the network to grab data. With the data in hand, the information can be read and further leveraged (i.e., using corporate passwords to access company intranets.)

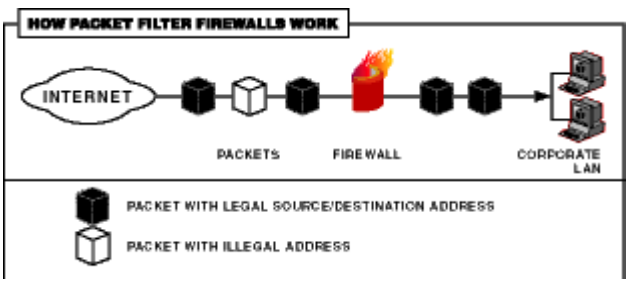
Using freely available software programs like the Security Administrator Tool for Analyzing Networks (SATAN), an intruder also can remotely grab network data being routed by network switches or hubs. This type of program exposes weaknesses in passwords and configuration that can be exploited by the intruder. These types of security issues make a strong argument for implementing a secure VPN capability in the corporate network.

Advantages and Limitations of Firewalls and Secure VPN Hardware Solutions

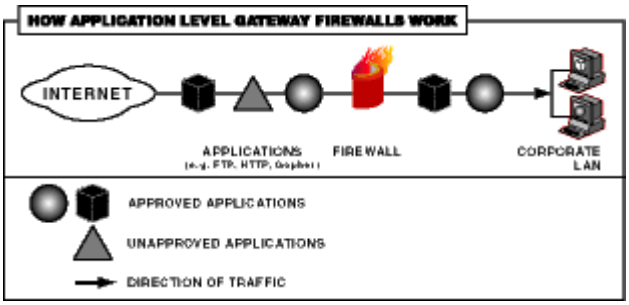
Firewalls
Firewalls have gone mainstream. The firewall market is expected to grow from $300 million in 1996 to $750 million in 1998 [4]. A firewall is typically software running on a computer or a series of computers that work together to create a barrier that prevents unauthorized access to sensitive corporate data (i.e., it keeps the "bad" guys out).

There are three main types of firewalls: packet filtering firewalls, application gateway firewalls, and stateful inspection firewalls.

Packet-filter Firewalls
Packet-filter firewalls are based on packet, or address filtering. These firewalls provide access control at the protocol layer, operating to accept, reject, or drop packets of data based on the source/destination computer network address and the type of application. The big advantage of this type of firewall is its transparency to the user and high-level transmission speed compared to other types of firewalls. The downside is that it provides only modest levels of security.



Application-level Gateway Firewalls
The second main type of firewall is called an application-level gateway. These firewalls impose access control restrictions at the application layer, such as e-mail, web browsers, or file transfer protocol (FTP). Application-level firewalls serve as a proxy for an external gateway server. The proxy establishes a connection to the external server on behalf of the internal user. This is a strength of these type of firewalls. Application gateway firewalls keep the private network configuration hidden from the outside and allows for a thorough examination of the data. Due to a reliance on application-level proxies that copy, examine, and retransmit data, application-level gateway firewalls are slower than packet-filter firewalls and therefore are not as transparent to the user.



Stateful Inspection Firewalls
The third category of firewalls is called stateful inspection firewalls. Stateful inspection firewalls use software engines to process application state information at the application layer of the OSI reference model. These firewalls begin by screening data packets against defined network access rules, like a packet filter. Packets that pass network access rules are then evaluated against the logical condition or state of the communications session and application associated with the packet. The firewall accepts packets that match the application's state and updates firewall state information changed by the packet. If a packet conflicts with the current state of the application, the firewall discards the packet.

In the latest releases of their products, firewall vendors have begun offering secure Virtual Private Network(VPN) services.[5] A VPN is defined as encryption and authentication combined to build secure tunnels over public and private networks. More information on VPNs is discussed in the next section.

What are the limitations of providing firewalls and secure VPNs? The encryption required for VPNs is a computationally intensive process because of the multiple mathematical calculations required to do the substitutions and permutations required to encrypt data. Combining this with complex firewall access control creates a bottleneck at the network gateway. Adding another compute-intensive process, like secure VPNs, can dramatically reduce performance. A 1996 International Data Corporation study identified maintenance of network performance as a key firewall feature.

firewall features.

Compounding the performance issue is the fact that, in order to save money, more and more firewalls are being shifted to less expensive Windows NT servers, which typically use Pentium (or Pentium Pro) processors. According to the RSA BSAFE (3.0 Benchmarks), an Intel Pentium-90 MHz microprocessor can run DES at 1 Mb/second. A standard T1 line operates at 1.554 Mb full duplex. The combined firewall and secure VPN encryption processing will create performance hits that slow the network gateway. Without a high-powered and expensive RISC-based UNIX server, wireline speed VPN encryption is not possible on a computer that also is hosting a high-performance firewall.

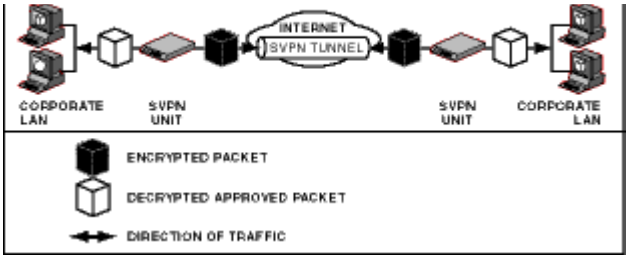
To summarize, firewalls are the security answer to protect the corporate gateway. Firewalls have proven to be a necessary foundation for sound network security. The are not an effective solution when building a secure VPN.

Secure VPN Hardware

Secure VPN hardware is not as easy to define as a firewall. To begin with, there are many names for this capability such as, standalone encryption hardware, network encryptors, crypto-accelerators, etc. Most people in the network security industry define VPN as a network that uses encryption and authentication to build secure tunnels over public networks. Some carriers consider the term VPN to also mean unsecured use of the Internet for corporate communications [8]. It is for these reasons that the word "secure" is added to the front of VPN to help differentiate it. As discussed earlier, secure VPN hardware devices use encryption and authentication to build secure tunnels with other authorized VPN devices over private and public networks like the Internet.

What do secure VPN hardware products do well? Bruce Schneier's book, *Applied Cryptography,* provides a good description of the advantages of hardware encryption.[9] Schneier writes, "Hardware [encryption] is the embodiment of choice for military and serious commercial applications. While some cryptographers have tried to make their algorithms more suitable for software implementation, specialized hardware will always win the race." Again, using data from *Applied Cryptography,* software 56-bit DES encryption on a dedicated 125-MHz HP 9000/887 microprocessor can operate at 12 Mbps. Hardware 56-bit DES encryption using a VLSI Technology VMOO9 with a 33-MHz clock can operate at 112 Mbps. By definition, hardware encryption is an order of magnitude faster than software encryption.

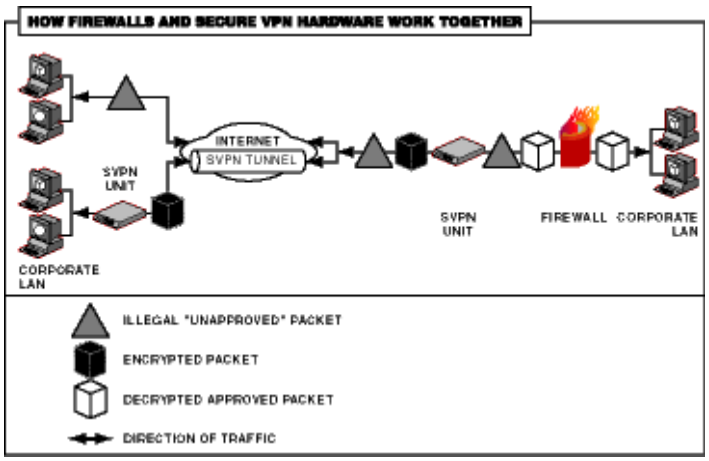
Because hardware can process items so much more quickly than software, secure VPN hardware devices are well suited for the computational intensities of encryption. This type of product typically operates at the network layer, application and operating system independent, and can drop transparently into the network.



How Firewalls and Secure VPN Hardware Devices Interoperate

If network performance is an issue for a multiple-office corporate network, the best combination for robust network security is a combination of firewall and secure VPN hardware: Secure VPN hardware providing wireline VPN encryption and firewalls providing thorough access control protection at the corporate point of entry.

So how do they work together? Most secure VPN hardware typically sits on a network between the router and the firewall. As described in the last section, these secure VPN hardware devices are designed to provide transparent privacy between, and authentication of, other authorized secure VPN units on the corporate network. Data communications traffic from locations without secure VPN units are passed in the clear directly to the firewall for its normal access control process. Traffic from remote sites using secure VPN hardware units are decrypted once it reaches the secure VPN hardware unit at the receiving location. The clear data is then passed to the firewall for standard processing. It is in this configuration that secure VPN hardware and firewalls work together for end-to-end corporate security.



Conclusions

Network bandwidth needs are increasing as corporations look to implement voice, video, and data over the same medium. As new multimedia applications come online, the requirement grows for new technology to secure these faster networks.

Simultaneously, budget-conscious corporations increasingly are looking to the Internet to either augment or replace leased lines. These corporations see secure

VPN capabilities as the means of obtaining cost-effective connectivity.

Increasing bandwidth requirements and the desire to control connection costs will require technology changes for firewalls and secure VPN hardware. Every person and corporation wants to be connected with the highest speed pipe. Given this, firewalls and secure VPN hardware will be part of the future solution, provided they are not a bottleneck on the network, and they provide the ability to save the corporation money through the use of the Internet. The combination can allow a company to not only be connected to the public services available on the Internet, but also offer a secure lower-cost alternative to interconnecting remote offices and users.

Footnotes

1. Choice Gets Less Remote—Dedicated hardware and server-based software widen remote-access options, *Information Week,* March 24, 1997
2. Forrester Research, 1996
3. FBI and Computer Security Institute Survey, 1997
4. Source: Wessels, Arnold and Henderson
5. ZD Internet Magazine *E-Print,* Find the Right Firewall, 1997
6. *Internet and Data Security,* Gerard Klauer Mattision & Company, December 1996
7. BASFE, 3.0 Benchmarks: An RSA Data Security Engineering Report, July 1, 1996
8. Virtual Private Networks: Safer Nets? *Communications Week,* March 17, 1997
9. *Applied Cryptography,* 2nd Edition, 1996, Bruce Schneier, Hardware Encryption versus Software Encryption, page 223.