Secure operating environments and their impact to bandwidth

White Paper provided by:
Dale Witt, Product Manger
NETSCREEN Technologies, Inc.
2860 San Tomas Expressway
Santa Clara, CA 95051

Introduction:

Emerging technologies are placing increased demands on corporate resources for access and throughput. The latency of data exchange is the result of two factors: 1) the number of requests, 2) the amount of data requested. The sum of these is typically identified as bandwidth and any manipulation of the data increases the latency and decreases the available bandwidth.

Security concerns present an opportunity for vendors and they must build the infrastructure to develop product and support the customer. The greatest return on investment for consumers and corporations will be in dedicated hardware, because the associated cost of ownership is low and current hardware is robust and reliable. The improvements in security software applications are predominately a function of advancements in server platforms.

Security Market Background:

In the current environment of corporations accepting distributed processing and moving away from central processing, security vendors can offer a variety of value-added services, predominately these are Firewalls and Virtual Private Networks (VPN). Further compounding this migration is the proliferation of personal computers, local area networks, collaboration, and software applications. These factors have created independent work groups with large data sets and services that are shared across time and distance. Considering additional factors such as contractors, alliances, consultants, and remote staff, the demand for bandwidth and security is growing at an exponential rate surpassing the ability of current security software applications to provide the bandwidth. Software applications typically reside on a general-purpose server and have evolved from legacy hosts, with marginal performance improvements, most of which can be attributed to advancements in the server platform.

Extranets increase options and competitiveness for businesses, associates and partners by sharing product, technical, and database information. All of which allow faster reaction, development, and delivery of goods and services to consumers and corporate customers, netting increased profit. All of these advantages in productivity and communications come with a risk, "who is looking at my data?" The eavesdropping on data is discomforting and an End to End private solution is needed on the public network to eliminate these concerns. Firewall and Virtual Private Network (VPN) technologies are currently the best solutions available.

The alternative choice has been for companies to sacrifice security for access, to the public Internet, allowing demand on corporate resources and information from anywhere and anytime. Corporate resources are accessed continually and processing is more distributed, files are larger and shared, growing the size of the operation, its complexity, and vulnerability. Content is authored and shared internally and externally by the company, associates, consultants, and remote staff. This approach offers WEB services, E-mail, electronic commerce, and location independent transactions, however these benefits come at a risk, the security of the data.

Market analyst have concluded and documented the size and demand for data, on the Internet, will continue to grow at an exponential rate, further stressing the bandwidth issue. The number of users, of the Internet, doubles every two years, exponential growth. This and the increasing amounts of data being transmitted are exceeding the current security solution's capacity.

If the data is secured, then an introduced delay and increase in file size is generally incurred, adding to the bandwidth dilemma. Offloading these security functions to efficient, high-speed, task specific, dedicated hardware engines is the most efficient and least costly solution available and is generally accepted as "state of the art".

In small and medium sized companies the IS function is commonly allocated to some one, who may not be completely qualified, as an administrator. The hardware accelerator is specifically designed and tuned, for a task, this action removes the responsibility and complexity from the administrator, who can be returned to core business functions that generate income. Typical saving for a company is 40-60% in the operating budget, with the adoption of VPN technology. Return on investment can be from a few weeks to months, dependant on the operation. The software application requires administration of the system, management, and the associated licensing of each user. Unfortunately most small companies can not staff an administrator for the system and security manager. Additional expenses are incurred for the operation and maintenance of a complex computer system.

Security Products:

Dedicated hardware vendors provide a family of intuitive, elegant, robust, reliable and competitively priced solutions for the small, intermediate, and fortune 500 sized business. These products provide corporations with security and performance, from a single vendor, that address Internet, Extranet, Intranet corporate services and remote access applications.

Products available, from hardware vendors, include function accelerators that integrate security products for corporations; including packet filtering, firewall, authentication, encryption, and VPN technologies, all in a single convenient and affordable package.

These products can be tuned and scaled to meet the immediate and future needs of the corporation with minimal intervention by the customer. The products are manageable by the customer or remotely by the vendor, where added value can be provided such as network performance monitoring, statistics, and reports. Remote access, from laptop applications, will be available for consultants, associates, and road warriors. The laptop applications will allow access, from anywhere, at anytime, and be easy to operate, with a robust feature set, reliable operation and comply with the emerging **IPSEC** standards.

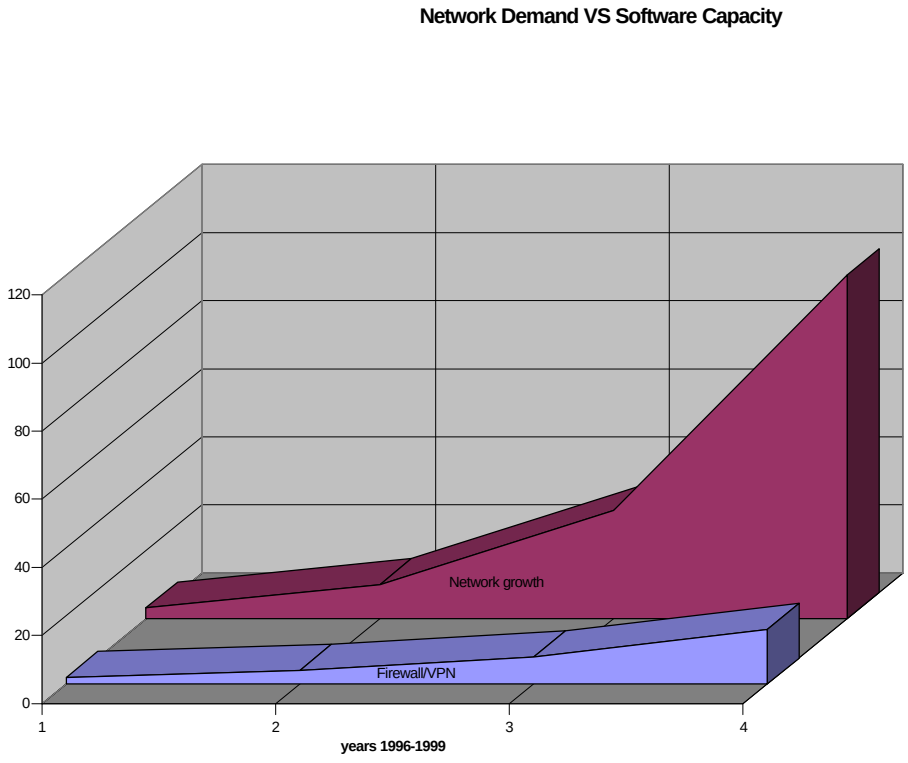
Dedicated hardware accelerator products will eliminate the concern about security; cost of leased lines, management of modem pools, and allows customers to focus on their business instead of security and network management.

Hardware Architecture:

Hardware has historically been more efficient than software at very specific, compute intensive, data manipulation tasks. Examples are 1) Floating-Point Processors, where the CPU passes the command and data to the unit allowing the CPU continues operations. 2) Graphic accelerators, where a library of macros can be called to perform specific manipulations of an image, while the CPU performs other tasks. Hardware that is task specific can operate with minimal intervention while a software application most always requires an operator, at the minimum, or a technical system administrator, more likely.

Figure 1: Represents the exponential demand for bandwidth and the available performance of Software applications, calibrated on the left side in Mbits and over four consecutive years 1996, 97,98,and 99.

Figure 1



The advantages of a "system" approach to the problem of Internet bandwidth and security is to parse the functions off into tasks that can be managed by the CPU and performed by specific components, most often an ASIC. In the architecture of the system RAM should be accessed by all system components, attached to any of the system's busses. Multiple internal busses allow parallel processing and access to the memory. The CPU can cache instructions and data, reducing the accesses to and from RAM. The ASIC can be given the instruction and the location in RAM of the operands and told to go, when complete the result is placed in a predictable location in RAM and the CPU is interrupted, with a DONE from the ASIC. The CPU is like an orchestra conductor who controls all of the instruments, but does not play. This allows each part to be dedicated to a task and become very efficient at that task. The parallel processing and task specific ASICs provide performance that was previously unattainable. The complete security solution will support a firewall to keep internal and external networks secure from attacks from both internal users and external hackers. Provide detection and alert, in the event of an attack, and defend against it. A defense is to have NAT or transparent IP addresses, which do not pass the address outside the firewall. VPN is a form of data transportation and traffic control with authentication of the user, encryption and inspection of packets.

Conclusion:

Security has been receiving increased attention from analysts, trade publications and there is an increasing demand for these products and services across all markets and company sizes. VPN is a data communication infrastructure available on the Internet with packet filtering, firewall, authentication and encryption securing the information transmitted. The VPN enables business to securely communicate with their associates, consultants, satellite offices, and employees using the public Internet.

Security technology has evolved beyond the early adopter phase and hardware accelerators currently offer robust feature sets that are intuitive, reliable and affordable. Security has entered the exponential growth portion of its life cycle and the demand for access, latency, and bandwidth is exceeding the capabilities of the current software applications to deliver security and throughput. The solution is a common industry approach, the dedicated hardware engine. Examples of this abound, Floating Point Processors, Graphic Accelerators, Networking Chip Sets, and Imbedded controllers.

System engineers and designers look to hardware for performance.