TeleChoice

NETSCREEN

The Opportunity and Requirements for Managed Internet Security Services

June 2000

Internet Security Market Overview

With the increasing desire to leverage the public Internet for the exchange of highly sensitive information, enterprises are now placing a far greater emphasis on the security solutions required to operate in such an open environment. Growth in the number and types of cyber-related crimes will unfortunately only continue. On a corporate level, these crimes range from the minor inconveniences of a prankster altering the content of a Web page to the major losses suffered from denial of service attacks that have been so highly publicized in the press as of late. The mechanisms enabling these cyber attacks continue to be enhanced, and holes in current enterprise configurations are recurrently detected and exploited, making security an ongoing concern rather than a one-time event.

In response to this growing need for corporate security, Internet firewalls and IP VPNs (Internet Protocol Virtual Private Networks) were created, continue to advance, and have become the security mechanisms of choice in the Internet community. An Internet firewall protects the private network infrastructure while allowing access to the public Internet and all of its resources. In essence, it is a device that controls access between networks based on information provided in standard data packets. It is typically thought of as providing perimeter security. For their part, IP VPNs establish secure communications between employees, branches, or partners by using strong IP-based encryption and authentication techniques—transport security. As a result of the security these components provide, enterprises are able to leverage the low costs of the Internet to provide a much cheaper alternative to traditional private network solutions such as leased lines, modem banks, and even frame relay.

The enterprise community initially took on the procurement, design, implementation, and management of these security tools itself. These early adopters typically had the internal staff, funding, and expertise to be on the leading edge. Still, many found it a complex undertaking and one that took them outside the focus of the core business. More recently, the trend among enterprises has been to seek out the assistance of providers under the umbrella of a managed security solution. The development of these offerings by service providers will prove particularly appealing to small and medium businesses that lack even more the internal resources required to secure their infrastructures. Some of the key security business drivers among these enterprises include:

- **Increasing Security Need.** As the Internet evolves toward true universality, an increasing number of businesses—across all sizes of organizations and industries—will seek to leverage the benefits this ubiquity creates and look to migrate more and more of their critical and confidential transactions to the public infrastructure. In its extreme form, the industry has already witnessed entire new business models predicated on use of the Internet as their sole domain.

- **Increasing Complexity.** IP networking in and of itself, much less securing access, can be an arduous undertaking. IP VPNs and firewalls represent highly complex solutions based on dynamic, changing technologies. New threats, exposure of vulnerabilities, and appropriate proactive measures can quickly become too cumbersome for an IT staff to manage. Add to this the constant state of change of today's enterprise network and the ongoing security threats this creates in the form of new security policies and considerations, and one has an environment ripe for outsourcing

- **Competition for IT Talent**. The growth of the Internet and related technologies has created a scarcity of IT labor in general. When good people can be found, it is usually at a premium salary and benefits, which drives up internal costs. This is especially true when the need is an area of particular expertise such as the security specialist, an even more expensive IT individual and one likely dedicated to the singular task of security management. As a result, managed security solutions will often deliver overall cost savings to an enterprise even with the additional fees associated with purchasing the service.

- **Pace of Industry**. In general, industry moves more quickly today and is increasingly competitive. Businesses are finding a growing need to focus on their core competencies and outsource non-core functions. This is true for small and medium businesses that outsource for cost/scale advantages as well as for large businesses (MCI WorldCom and AT&T both outsource IT functions).

Obviously, the Internet offers an attractive solution and opportunity in the way business can be conducted and in the way businesses operate. Security is a lynchpin in ensuring the business Internet's success, and it is more and more apparent that many enterprises will require the assistance of providers to deliver on the Internet vision. Managed security solutions— managed firewalls, managed VPNs, virus scanning, URL filtering, intrusion detection—offer the service provider an attractive opportunity to differentiate itself, increase revenues, and more importantly, increase the level of the relationships it has with its customers.

Why offer managed security solutions?

- The market potential for managed security is growing exponentially.
- Customers are demanding and budgeting for security outsourcing services.
- Higher-value services lead to increased profitability.
- Customer retention increases as customers purchase more services from a single provider.
- Selling multiple services to a single customer means increased revenue per customer.
- Service providers are likely already to have some of the necessary security talent in-house.
- Managed security will lead to other product sales such Web hosting services.
- As customers build Extranets, there is the opportunity to sell to their business partners.
- The competition is offering managed security services.
- Helping customers to meet their business objectives is a much more strategic position for a service provider than merely providing them with bandwidth.

Security Components

But what does securing the Internet entail? In the broad sense, security encompasses elements ranging from physically securing the network and equipment to securing the data storage itself. From the perspective of a service provider, the key element for security is the network layer. Security of the network layer can be viewed in two arenas: access control and secure transit. Access control secures the perimeter and demarcation between the end user's private network and the public Internet. It determines what goes out and what comes in and is currently addressed through firewalls. Secure transit essentially means protecting data in transit over the public Internet. Today various types of encryption schemata address this need through IP VPNs.

The four goals of security:

1. **Confidentiality.** Only the sender and receiver can read messages.
2. **Authentication**. Messages are indeed from the expected originator.
3. **Integrity.** Messages have not been altered in transit.
4. **Non-Repudiation.** Contracting parties cannot "back out."

Although the security focus here is on firewalls and VPNs, it is worth mentioning that the term "Internet security" can refer to a wide range of products and services, and service providers entering this market may choose to offer a comprehensive portfolio of services including:

- **Firewall Management.** Firewall management often includes providing security equipment and Internet access as well as services such as installation, configuration, remote monitoring, usage reporting, version control, and alarms notification.
- **Managed Virtual Private Networks.** Managed VPNs are viewed by many as an alternative to traditional enterprise data services such as frame relay and private lines. They utilize encryption to transmit data securely.
- **Security Training.** Internet business customers believe that service providers are a credible source of information on security matters. Offering to train customers on security threats, recognizing attacks, and security measures is a valuable means of establishing customer relationships.
- **Security Needs Assessment.** This is a service whereby a security expert reviews an organization's policies, procedures, and security implementation to assess the viability of the organization's defenses.
- **Intrusion Detection.** Intrusion detection consists of various methods of determining if an inappropriate access attempt is made. Common attack methods are documented and inspection techniques incorporated to defend against them.

- **Vulnerability Assessment.** Often performed as part of the needs assessment, the simulated attack involves testing an organization's security implementation to identify vulnerabilities. Tests are conducted using the same methods real-life hackers use to find holes in a secure network.

- **Security Policy Development.** Security policies include everything from how diskettes and laptops are maintained to the exact configurations of firewall devices and routers within a network. An organization's security policy should be developed to balance its business needs with its requirements for information security.

Internet Firewall Services

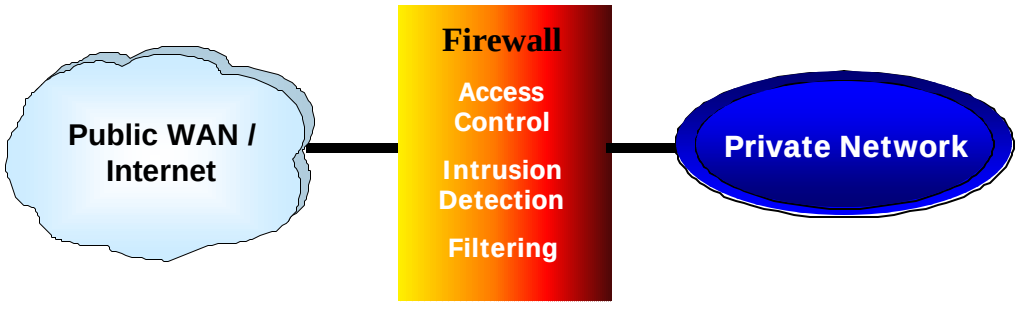
To put it simply, the Internet firewall is designed to keep the bad guys out, let the good guys in, and keep the good guys from going to the bad guys' sites. There are many firewall topologies or architectures deployed today ranging from basic access control (filtering) on routers to multi-tiered levels of firewalls on isolated network segments.

- **Packet Filters.** Packet filters use information in the IP packet header (network layer 3) to make access decisions. Information used to filter may include source IP address, destination IP address, upper-layer protocol, or protocol port number. Packet filters will allow a packet to pass if it meets certain criteria or will drop a packet if it does not meet security criteria. Because packet filtering is a low-level process, it can be accomplished very rapidly.

- **Application Proxies.** Application proxies are firewalls that make access decisions based on information contained in the TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) header. TCP and UDP are the layer 4 protocols commonly in use on the Internet. These firewalls are known as proxies because traffic traveling from the user side to the Internet side is actually replaced with a new IP packet; no IP packets are allowed to pass directly from user to Internet. From the Internet side of the application proxy, it looks as if all traffic from that location is originating from a single host.

At one point debates on these architectures could reach religious proportions; however, with the maturing of the technologies, vendor solutions have advanced considerably while costs have significantly decreased. Today there is little need for even small and medium enterprises to compromise on a solid security architecture.

A basic sample configuration would appear as depicted below:



So what is a firewall protecting against? As mentioned previously, the number and types of cyber attacks continue to increase. Here are a few example categories with which the enterprise customer is concerned:

- **DoS (Denial of Service).** This is a general term describing any intentional means of disrupting network services under the guise of seemingly normal connections. The perpetrator will use either a direct attack from a remote site or launch a distributed attack from multiple sites, usually unbeknownst to the attacking host. The attacks result in either a consumption of significant system resources or an outright crash of systems—both of which cause service outage to legitimate users. There are many specific types of DoS attacks, which can fall into several categories:

  - ✓ **Connection Floods.** Requests for TCP connections to initiate a legitimate service (Web, FTP, etc.) open SYN ports, filling the available resources for allocation. This is like parking empty cars at the drive-in—spaces are taken but no orders are placed and legitimate customers must wait or drive to the next establishment.

  - ✓ **Ping Attacks.** Called "smurfing" or "ping of death," multiple ping commands (ICMP packets) are sent with a forged source address to another networked device. The device autoreplies to the forged initiator, which in turn echoes the request. A storm of packets is created and traffic slows significantly, effectively denying service for legitimate users.

  - ✓ **Process Table Floods.** Various processes or daemons that listen for connections and then spawn the appropriate process can be duped into launching more processes than will fit the UNIX system process table. These attacks differ from connection floods as they not only tie up service but also cause a system to crash abruptly, making for lengthy rebooting, potentially lost data, and longer outage time frames.

- **Hijacking Resources.** Here the hacker stages or steals enterprise resources to launch his/her attacks on other systems/enterprises.

- **Vandalism.** This type of hacking involves the prankster who for fun corrupts corporate data and/or defaces the enterprise's website.

- **Stealing Identifications.** Where the previous attacks mentioned are most definitely an annoyance to the enterprise, an attack in which identifications/passwords are stolen for use in gaining access to company confidential information is a scenario that keeps an IT manager awake at night.

Managed Firewall Services

The importance placed on the controls involved in properly operating a firewall has led service providers to offer outsourcing services. Managed firewall services generally consist of maintaining and operating a firewall owned/installed by the customer or service provider on the customer premises. This firewall is either a software-based application residing on a UNIX or NT server, or it is a specialized hardware solution. Specialized hardware solutions continue to come down in price and, combined with their "bullet-proof" architecture design and high levels of performance, are gaining in popularity across all enterprise segments. Regardless of the configuration specifics, firewalls generally perform access control functions through a series of rules or conditions. Under a managed solution, service providers assist enterprises in designing, implementing, and maintaining these rule sets. Key components are outlined below:

- **Access Control.** Broadly defined, access is controlled on the following levels:

  - ✓ **User.** Specific user names and passwords can be assigned to limit access on a user-by-user basis.

  - ✓ **IP Address.** Specific host addresses are regulated for incoming and outgoing traffic. A database server, for instance, may be restricted from both outgoing and incoming traffic.

  - ✓ **TCP/IP Service.** Each IP service utilizes a specific TCP (Transmission Control Protocol) port for establishing a session. For example, Web servers typically use port 80 for HTTP traffic. The firewall rule set may allow all outgoing requests for internal users to connect to port 80 on remote websites but will limit incoming port 80 to a system(s) designated as a Web server(s).

  The service provider works with the customer to establish these rule sets, generally starting from a standard configuration and then applying the appropriate customization for each customer.

- **Packet Inspection and Filtering.** This is an analysis of the data packet's source, destination, and in some cases, content. "Stateful" inspection of packets is analysis of packet header information in the context of its transmission (i.e., whether it is a return packet, originating packet, or another connection to/from the source/destination).

- **IP Address Management.** The firewall will generally support the following address management services:

  - ✓ **NAT (Network Address Translation).** NAT is performed primarily for two reasons: 1) a customer may be using an unregistered set of IP addresses on the internal network, addresses that will not be routed over the public Internet, and 2) a customer may want to hide internal addresses for additional security.

  - ✓ **DHCP (Dynamic Host Configuration Protocol).** DHCP automatically assigns IP addresses to individual clients. This allows great flexibility in the configuration of workstations, especially for mobile users.

- **URL Filtering.** URL filtering blocks access to undesirable websites. Various subscription services exist to provide this capability, which is often packaged within a service provider's managed solution.

In addition to the management/maintenance of core firewall components, typical management services offered in conjunction with a service provider's managed solution today include:

- **Monitoring.** From a central location (NOC) the service provider monitors security alarms and events on a 24 x 7 basis. Typical monitoring capabilities include:

  ✓ Device health.

  ✓ Connectivity status.

  ✓ Network traffic throughput.

  ✓ Network traffic by application type (HTTP, FTP, etc.).

  ✓ Failed logins.

  ✓ Blocked packets.

  ✓ Attempted intrusions.

- **Maintenance.** Maintenance entails day-to-day and periodic upkeep of the system hardware and software for the customer solution. Options may include on-site repair, 24 x 7 coverage, and four-hour maximum time to respond on site.

- **Reporting.** Service providers offer detailed reporting not only on security events/alarms but also on Internet usage, performance measures, etc. Specific examples include:

  ✓ Current firewall policy snapshot.

  ✓ Tickets (time opened, time closed, and action taken).

  ✓ Session logs (can be filtered to report only defined threshold events).

  ✓ Internet connection performance (availability, throughput, and other parameters).

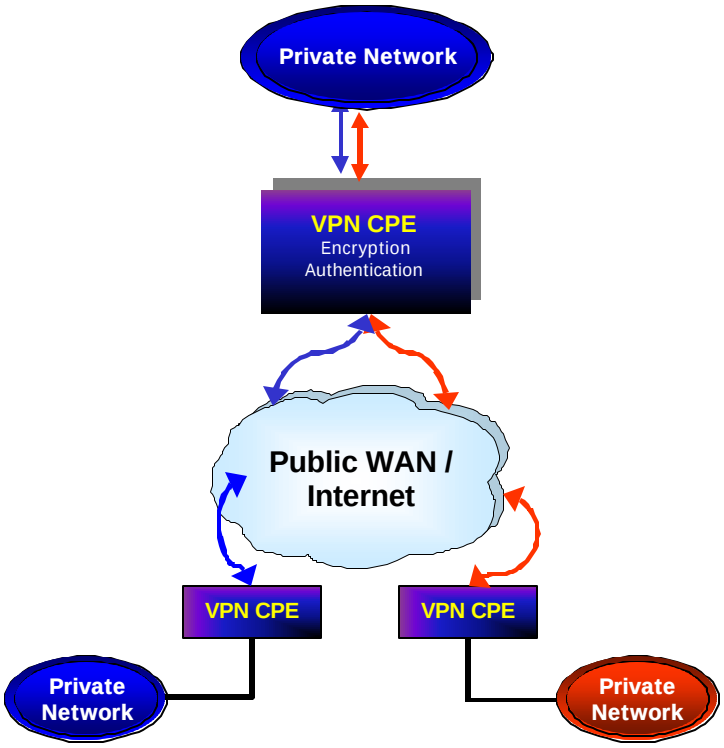
  ✓ Intrusion attempts and anomalies.

IP VPN Services

IP VPNs support private communications over a public network, such as connecting two users or network locations over the Internet. These solutions often dictate that security measures be inherent to the service. Today IP VPNs are typically viewed as falling into three major categories: remote access VPNs, Intranets (company site-to-site), and Extranets (business-to-business). These services are now being adopted by companies of all sizes as a result of the powerful combination of high-speed access links and public networks. An example is the use of high-speed, low-cost broadband DSL connectivity to enable teleworkers to link securely with the company network via the Internet, as if they were accessing the LAN at the office.

IP VPNs can offer several advantages to both the end user and the service provider. A service provider can leverage a public network while positioning its services to support end-user applications. End users typically save money, sometimes in monthly charges and other times in reduced management of the network and its equipment. For example, with VPNs, many end users are able to eliminate modem banks and remote access server software for dial-in users.

A sample VPN configuration would be as follows:



Enterprises initially built IP VPNs themselves by purchasing the requisite security and routing equipment and only access and/or transport from a service provider. The day-to-day management and maintenance responsibility, therefore, fell to the enterprise itself. In offering a managed IP VPN service, the service provider takes on much of the design, CPE procurement, installation, change management, maintenance, and ongoing monitoring on behalf of the enterprise.

Today, service providers enable VPNs via hardware or software located at the customer's premises, which the service provider manages. These devices or solutions utilize technologies such as tunneling, encryption, and authentication to ensure secure communications across a public infrastructure.

Tunneling

Tunneling encapsulates one type of data packet into the packet of another protocol. IP VPN tunneling adds another dimension to the tunneling procedure in that before encapsulation takes place, the packets are encrypted so the data is unreadable to outsiders. Once the encapsulated packets reach their destination, the encapsulation headers are separated, and packets are decrypted and returned to their original format.

Multiple tunneling protocols are used today on the market:

- **PPTP (Point-to-Point Tunneling Protocol).** PPTP includes compression and encryption techniques. This protocol was introduced by Microsoft to support secure dial-up access for its desktop, which corresponds to a large share of the desktop market.
- **L2F (Layer 2 Forwarding).** Introduced on the market by Cisco Systems, L2F was primarily used to tunnel traffic between two Cisco routers. It also allows IPX traffic to tunnel over an IP WAN.
- **L2TP (Layer 2 Tunneling Protocol).** L2TP is an extension to the PPP (Point-to-Point Protocol) and merges the best features of two other tunneling protocols: L2F and PPTP. L2TP is an IETF (Internet Engineering Task Force) emerging standard.
- **IPSEC.** This is a collection of security protocols from the Security Working Group of the IETF. It provides ESP (Encapsulating Security Payload), AH (Authentication Header), and IKE (key exchange protocol) support. This protocol, mature but still technically in a draft format, is currently considered as the standard for encryption and tunneling support in VPNs.

Encryption

Encryption is the marking, transforming, and reformatting of messages to protect them from disclosure and to maintain confidentiality. The two main components of encryption are algorithm size such as Triple Pass DES (112 bits), RCA (128 bits), and Triple DES (168 bits), and management of the distribution of keys (IKE and PKI). These more recent key sizes greater than 100 bits have been a major driver in the success of IP VPNs due to their strength. They make it extremely difficult to hack into enterprise computer systems without an investment of millions of dollars in equipment.

Encryption starts with a key exchange that must be conducted securely. The IKE (IsaKamp OaklEy) protocol has been considered the most robust and secure key exchange protocol in the industry to date. It is also considered as a de facto standard for service providers and product vendors requiring the highest level of security for their VPN solutions. PKI (Public Key Infrastructure) is new to the key management scene and is currently thought to be the long-term solution to simplifying the management of VPNs. The industry is still evaluating and testing PKI with some initial deployments beginning to occur.

From an IP VPN performance perspective, encryption is a CPU-intensive operation. As a result, enterprises must evaluate (or service providers on behalf of the enterprise) VPN products in two primary areas as they relate to encryption. The first is whether the maximum throughput decreases substantially when encryption is used, and the second is whether or not a consistent throughput can be maintained when encryption is enabled. Typically, the likely tradeoff between performance and price is debated from a software- vs. hardware-based encryption perspective.

Authentication

Authentication methods define how IP VPN units validate the identity of other components. It ensures that a party or device is who or what it says it is. There are various authentication technologies that can be utilized for IP VPNs, the most common being RADIUS, tokens, and digital certificates. When it comes to choosing an authentication platform from the enterprise's perspective, the biggest considerations include security and cost of implementation and support. The latter is a major driver for enterprises considering a managed solution.

Digital certificates are fast becoming the preferred authentication choice in the market, mainly because of better overall security and universal authentication of user features. Corporate IT managers list better security, ease-of-use, universal authentication, privacy, partner's needs, secure e-commerce, and remote access as the key drivers for choosing digital certificates. However, many customers do not require this level of security, particularly as the implementation costs can often be high. When customers do not have the financial resources or simply the business need for digital certificates, RADIUS and LDAP (Lightweight Directory Access Protocol) are the methods of choice.

Customer Requirements

What do customers look for in a managed security solution? Security, performance, scalability, pricing, and management are the most frequently used criteria. General security guidance is also highly regarded as small and medium businesses begin to make their way through the security maze. Small and medium businesses are seeking answers to questions such as:

- How much security do I really need?
- What types of security measures do I need?
- What skills are needed to manage security installations?
- How do I make sense of all the standards and technologies involved with network security?
- What will I need to spend to ensure the security of my data?

- Will the security equipment I want to purchase work with my service provider's network?
- At what point in my network should security measures be implemented?
- What is the right tradeoff between security, speed, and price?
- What kinds of people and resources do I need to develop and implement my security policy?

Security

For most IT managers, a solid security policy must include data encryption, user authentication, and firewalls. Additional tools such as reporting (for audit purposes) and documented security policies are also often required to complete security measures.

Small businesses are usually more sensitive to costs when defining their security policy. As a result, they tend to opt for slightly less secure but more economical solutions:

- For economic reasons, software-based encryption has historically been the preferred choice for sending encrypted traffic. However, the advent of firewall/VPN CPE presents a lower-cost alternative to the traditional, more costly software-based systems.
- RADIUS-based authentication as opposed to digital certificates.
- May be considering a router-based packet filter as opposed to a dedicated firewall due to costs.
- Will rarely implement a security policy or audit security logs, partly because they do not consider themselves as primary targets for Internet hackers.

Service providers are only now beginning to consider the security needs of these small businesses. As a result of more cost-effective solutions/devices, service providers will be able to package robust offerings at attractive prices previously unavailable to this market.

The medium and large business segment typically requires a more robust solution. The medium-business customer implementation is highly dependent upon on budget availability, criticality for secure communication, and the current state of networking. If requirements are on the low end, the medium business will consider the cost/security tradeoff, and if requirements are on the high end, it is likely to select the full-security approach. In addition to the fact that a larger number of sites must be equipped, medium and large businesses systematically look for the best security practices available:

- Digital certificates or hardware authentication.
- Hardware-based encryption with Triple DES and IPSEC tunneling.
- A firewall, well-documented security policies, access to audit security logs.
- Proactive monitoring of the firewall/VPN/Internet activity.

Performance

Performance is a close-second priority in the eyes of IT managers. Performance is addressed with SLAs that typically cover packet dropping, latency, and network availability, or port availability for a remote access service. It is essential to emphasize the importance of evolving QoS techniques as a foundation to SLAs. These tools are bringing predictability and reliability to today's IP networks and will make possible the definition of classes of service that will deliver priority service.

Robustness of the firewall/VPN equipment is also of particular importance regarding performance in the eyes of the enterprise. High and consistent throughput, low packet loss levels, and redundancy capabilities are purchase factors for the equipment portion of managed solution bundles.

Scalability

Scalability, in the context of a secure IP service, refers to seamlessly adding new sites to a VPN, new services/rule sets to a firewall, and augmenting the number of users. Ease of use and flexibility to scale a firewall/VPN in these areas are key decision criteria for many enterprises evaluating managed providers.

Pricing

IP VPNs are touted by the industry as delivering substantial cost savings when compared to other WAN solutions. Managed firewalls can also reduce overall internal costs for enterprises. Compelling pricing can be a determining factor in the decision process, particularly for the lower end of the market. Nevertheless, the importance of security and performance encourages many customers to accept higher prices as long as there are convincing levels of security and performance guaranteed, for example, in SLAs.

The most popular pricing model for outsourced security services is a monthly recurring fee and a one-time installation charge. The market has not yet delivered a clear reaction to a usage-based VPN model, although some argue that it is as an additional way to reduce overall costs. At best, it is considered an interesting option by some enterprises but not to the point of impacting the provider evaluation process.

Management

Companies seeking outsourced firewall/VPN capabilities from service providers feel they can focus on serving their internal customers rather than dealing with constant transformation and troubleshooting.

IT managers typically look for the following management features in a service provider offering:

- **Network Security.** Network security involves the management of all network security components, except in some cases the management of user profile and authentication.

- **Network Audit.** Network audits create reports that can be accessed by customers on a password-protected website.

- **Tailored Reporting with SNMP, Historic Data, and Tickets.** This information can be accessed through a password-protected website.

- **Security Design.** This involves the creation of an architecture covering physical, network, system OS, and application layers of security.

- **On-Site Replacement of Equipment.** If hardware fails, a technician is dispatched to replace it.

- **Role-Based Management.** Role-based management provides flexible solutions for shared management between the service provider, the customer's network administrator, and other individuals with specific management rights.

Looking Ahead

Due to increasing demands for security services across the scope of enterprises, managed security services including firewalls and IP VPNs will become table stakes for the service provider. Creating an attractive solution package is heavily dependent upon the individual needs of the market targeted, with a one-size-fits-all approach unlikely to find success. Service providers who have not entered the space should now look to enter the market addressing the security components previously discussed with plans outlined for evolving as the enterprises evolve.

An interesting result of enterprise demand for security services and service provider desire to take advantage of this demand with managed security solution packages, is the evolving segment of wholesale managed security providers. Many retail service providers targeting the small and medium business segment are realizing the opportunity before them in the way of adding value-added security services to their access offerings, but they lack the internal expertise, support tools/infrastructure, and staff to do so. Wholesale-focused managed security providers enable these organizations by offering prepackaged security components that can be private-labeled. All of the behind-the-scenes support, monitoring, and maintenance are provided by the wholesaler on behalf of the retail provider.

Going forward as the VPN market continues to mature, enhancements such as various QoS levels will begin to emerge as additional customer requirements. Enterprises should be expected to require more sophisticated solutions of providers as they themselves become more familiar and comfortable with the technologies. The managed security space has matured to a point where revenue opportunities are available to many-sized service providers targeting various-sized businesses but not yet to a point where the most advanced technology solutions are required to compete or succeed, especially in the small- to medium-sized enterprise.

About Telechoice

TeleChoice is a market strategy consultancy for the telecommunications industry. Supporting service providers and equipment vendors, TeleChoice focuses on leading edge public network technologies. Since Danny Briere founded the company in 1985, TeleChoice has been differentiated by its proven ability to transform new technologies into successful products and services. Its portfolio of offerings helps our clients conceptualize, launch, market and exploit the telecommunications market -- faster, more efficiently and more profitably. TeleChoice has been integral to the design and implementation of over 200 network services worldwide. The many "firsts" TeleChoice consultants have deployed include: Frame Relay Service; Managed Firewall Service; ATM Service; Managed Data Service; ATM-based LAN-WAN Service; and ADSL Service. More information on TeleChoice can be found at http://www.telechoice.com.

About NetScreen

NetScreen Technologies Inc. develops ASIC-based Internet security appliances and systems that deliver high performance firewall, VPN and traffic shaping functionality to e-business sites, broadband service providers and application service providers. This offers customers record-breaking wire-speed performance, scalability, and manageability in one comprehensive security solution. NetScreen sells exclusively through strategic partners such as Equinox Solution Through Partnership, Hitachi Seibu Software, Patriot Technologies, Inc., and WebZone Inc. More information on the company and its products can be found at http://www.netscreen.com or by calling toll free at 1-800-638-8296.