Internet & Network Security Solution Provider

BUSINESS PLAN

SAFETY NET CANADA, INC.

8789 Elk Avenue
Vancouver, British Columbia V3N 4E9
Canada

Safety Net Canada wants to become the dominant provider of a reliable, impervious, easy-to-use Internet and network security solution to corporate and retail customers worldwide. This plan raised over $5 million (U.S.) for the company and was written by Concord Business Development Inc. of Vancouver, British Columbia.

HIGHLIGHTS

Mission Statement

Safety Net Canada will be the dominant provider of a reliable, impervious, easy-to-use, and cost-effective hardware- and software-based, Internet and network security solution to corporate and retail customers worldwide.

Industry: Technology-Internet and network security.

Singular Features

Safety Net Canada will be the first network security company to introduce an information security solution that meets all criteria for reliability, compatibility, ease-of-use and scalability.

Target Market

Safety Net Canada identifies four target market segments for its Security™ line of network security products: large organizations, small and medium enterprises, and individual consumers.

Regional Expansion

Safety Net Canada will build its market share by gradually entering all major international markets by the end of the planning period subject to this plan.

Revenue Streams

The revenue model of Safety Net Canada comprises a primary and a secondary revenue category, with each category containing multiple revenue streams derived from the different Security™ models.

Capital Requirements: US $5 million.

Use of Proceeds

To complete product development and pre-launch testing, build and launch the website, launch marketing and promotion programs, build an administrative infrastructure, and acquire human resources.

EXECUTIVE SUMMARY

Corporate Vision

Safety Net Canada is based on the philosophy of growth. The company is dedicated to continuously innovating and expanding its line of security products in order to meet the needs of a dynamic and rapidly growing networked population. The management's vision for long-term sustainable growth incorporates the creation of a stimulating and creative corporate environment. Within such an environment, the members of Safety Net's talented team have the opportunity to continually enhance their individuality and creativity while contributing to the growth and long-term success of the company.

Products

Safety Net Canada will be the first network security company to introduce an information security solution that meets all criteria for reliability, compatibility, ease-of-use, and scalability. The flagship product line is comprised of two components: the Security™, a hardware device that protects computers from intruders, and the Security Guard™, complementary firewall and anti-virus software to protect the operating system and applications. By working in compliance and complementing each other, these two products amalgamate into a bulletproof network security solution that is resistant to currently known loopholes in security hardware appliances and software.

Market Opportunity

The Internet and network security industry is a rapidly growing segment of the high-tech business sector, as businesses and individual consumers become more aware of the security threats caused by conducting transactions and exchanging information in a networked environment. Internet and network security is currently a US $5 billion business, growing two-fold from its 1998 level of US $2.3 billion. North America and Western Europe account for 84 percent of all 1999 network security sales, with North America at more than

two thirds of total sales worldwide. Network security sales revenue is expected to grow even faster over the next three years, as Internet and broadband adoption, as well as e-commerce, continue expanding worldwide.

Security is not just for insurance purposes anymore but is an important part of corporate policy and strategy. The Internet is a source for increased profitability, and companies need sophisticated security solutions to expand trusted relationships with their customers, partners, suppliers, and channels. This need is the vehicle of the network security market. According to IDC, its worldwide revenue will jump from less than $4 billion in 1999 to more than $11 billion in 2004.

Safety Net Canada will take advantage of the vast profit and market share potential in the industry by being the first-to-market supplier of a complete network and Internet security solution, targeted at both organizational and individual clients.

Marketing Plan

Building a strong corporate and retail customer base and developing a high industry image and profile are corporate-level objectives subject to the company's marketing and promotional efforts. Each of these goals will be pursued and achieved through the implementation of an array of marketing and promotional actions geared towards fulfilling the directives of Safety Net Canada's marketing plan.

The Security™ product line will be rolled out into all four target market segments simultaneously. Different blends of distribution channels and marketing techniques will be used to reach the various market segments.

Safety Net will build its market share by gradually entering all major international markets by the end of the planning period subject to this plan.

Strategic Alliances

Safety Net plans to form strategic alliances with large hardware equipment manufacturers and anti-virus software companies as part of its plan to pursue an expansionary corporate level strategy through vertical integration.

Competition Summary

As the Internet and network security industry is projected to grow, the competitive environment will become more heated. Competition will ensue from both incumbent companies and new entrants. Established technologies, such as firewall software, will be subject to downward price pressure and low-cost competition. The competitive rules for newer information security technologies, such as Gap Technology appliances, will continue to be derived from product innovation rivalry and differentiation.

Safety Net Canada has no direct and two close indirect competitors for its complete Security™ solution. None of the company's other industry rivals offer a software and hardware-integrated, off-the-shelf, and easy-to-use security product.

Competitive Advantage

Safety Net Canada's competitive advantage is two-dimensional. One aspect of it is the company's ability to differentiate its products based on core competencies-innovation in product development and superior customer service. The second source of competitive advantage is cost-efficiency, with Safety Net Canada being the sole player in the Internet and network industry able to deliver a multi-faceted, reliable security solution at nominal cost. Long-term sustainability will be achieved through continuous innovation and customer service improvement.

Management Team

Safety Net Canada's management team is composed of skilled executives and Information Technology experts with previous experience in the Internet and network security industry. Other areas of expertise include market assessment, hi-tech research and development, as well as business venture formation and development. These individuals possess the superior determination, clear vision, and exceptional experience key to the success of the company.

Revenue Streams

The revenue model of Safety Net Canada comprises a primary and a secondary revenue category, with each category containing multiple revenue streams derived from the different Security™ models:

- **Sales through Distributors** -Revenues derived from distribution network sales contributes up to 70% of total revenue.
- **Direct Sales** -Revenues derived through the direct sales channel comprises approximately 30% of total revenue.

Capital Requirements

To deliver on its business proposition and take advantage of the existing opportunities in the marketplace, Safety Net Canada is seeking to raise US $5 million. Proceeds will be used to complete flagship product line development and pre-launch testing, build and launch the website, launch preliminary marketing and promotion programs, build an administrative infrastructure, and acquire human resources.

COMPANY OVERVIEW

Vision

Today, the increasing volume and speed of information exchange is accompanied by an increased potential for data to be manipulated in various ways including illegal tampering, altering, theft, or destruction. Safety Net Canada has been created out of the vital need of consumers and business users to have complete and reliable protection of information exchanged via public and private networks. The company is dedicated to continuously innovate and expand its line of security products in order to meet the needs of a dynamic and rapidly growing networked population.

Safety Net Canada is based on the philosophy of growth. The management's vision for long-term, sustainable growth incorporates the creation of a stimulating and creative corporate environment. Within such an environment, the members of Safety Net Canada's talent team have the opportunity to continually enhance their individuality and creativity while contributing to the growth and long-term success of the company.

Goals

Safety Net Canada resolves to treat customers, stakeholders, and the community with fairness and respect. These groups see the company as providing a sound financial return on investment, a robust, state-of-the-art Internet and network security solution, customer service and support, and a commitment to economic growth within the community.

Corporate Objectives

Management believes that following a preset strategic course, leading to a clearly defined set of enterprise-wide objectives, will result in increased shareholder and stakeholder value and foster revenue and organizational growth. In line with its corporate mission, vision, and long-term growth strategy, Safety Net Canada will pursue the following fundamental corporate objectives:

- To position Safety Net Canada as a predominant leader in the Internet and network security industry
- To maximize shareholder and stakeholder value by growing the company and its revenue
- To keep innovating and testing new technologies in order to keep pace with the global demand for security

Short-Term Functional Objectives

Successful implementation of the company's business model requires accomplishment of the following short-term functional-level goals:

Product Development

- Creation and maintenance of an effective distribution system with sales of up to 70% of total revenue
- Successful launch of the Security™ flagship product line by the end of Q1 2001
- Initial design of fingerprint authentication technology and prototype development of the 1020 Security™ scrambler by the end of year 2001

Marketing and Sales

- To dominate the North American market, develop the Asian market, and penetrate the European and South American market by the end of year 2003
- To grow sales revenue from US $5.4 million in year 1 to US $62.5 million in year 3
- To develop a worldwide brand name by the end of year 3

Business Development

- To secure corporate allies for the manufacturing and distribution of the Security™ by mid-Q1 2001
- To utilize and sustain long-term competitive advantage based on differentiation through product and service innovation

Strategies

To accomplish the objectives of its short-term and long-term planning periods, Safety Net Canada will follow a predetermined set of strategies at the corporate and business levels.

Corporate-Level Strategy

Safety Net Canada will pursue an expansionary enterprise strategy, based on vertical integration through strategic partnerships with large hardware OEMs and leading security software companies. Through these partnerships, the company has the opportunity to explore the profit potential of its trademarked technology while limiting competitors' access to international distribution networks.

Business-Level Strategy

With its patent-pending status, Safety Net Canada's competitive advantage is rooted in differentiation through innovation. The patent pending allows the company to harvest profits from commercializing the technology. To sustain its competitive edge in the long run, Safety Net Canada will continue investing in new product development. To lock out competitors, the company will trademark all new and unique technologies developed in the future.

Corporate Data

Date of Incorporation	June 16, 2000
Name of Incorporation	Safety Net Canada Incorporated
State of Incorporation	Nevada, USA
Principal Place of Business	8789 Elk Avenue Vancouver, BC V3N 4E9
Telephone	(604) 588-7565
Fax	(604) 575-6415
E-mail	info@safetynet.com
Website	www. safetynet.com
Fiscal Year End	September 30
Corporate Accountant	Samual Tom
Corporate Attorney	Jensen Devil Barristers and Solicitors

Date of Incorporation	June 16, 2000
Name of Incorporation	Safety Net Canada Incorporated
State of Incorporation	Nevada, USA
Principal Place of Business	8789 Elk Avenue Vancouver, BC V3N 4E9
Telephone	(604) 588-7565
Fax	(604) 575-6415
E-mail	info@safetynet.com
Website	www. safetynet.com
Fiscal Year End	September 30
Corporate Accountant	Samual Tom
Corporate Attorney	Jensen Devil Barristers and Solicitors

Proprietary Technology

The company has a granted patent pending in North America and has applied to trademark its Security™

technology under the Patent Co-operation Treaty (PCT). Under this treaty, Safety Net Canada maintains exclusive rights to sell manufacturing rights for profit in North America and more than 90 other countries worldwide.

Management Team

Safety Net Canada's management team is composed of skilled executives and information technology experts with previous experience in the Internet and network security industry. Other areas of expertise include market assessment, hi-tech research and development, as well as business venture formation and development. These individuals possess the superior determination, clear vision, and exceptional experience key to the success of the company.

Safety Net Canada will continue acquiring new and creative individuals in order to complete the personnel requirements of its managerial and corporate structure. The company's management team will be gradually completed as new executives are interviewed and appointed to fitting positions, according to the company's hiring procedures.

Vicki Smith-President and CEO

Ms. Smith has extensive experience in business development in the Internet and network security industry. Before coming on board with Safety Net Canada, she was the active leader of New Wave Technologies-a network administration and support consulting company. During her four years of involvement with New Wave Technologies, Ms. Smith managed to build a substantial client base composed of small, medium, and large corporate customers throughout North America.

Ms. Smith wrote her first computer program at the age of 14, has a B.Sc. degree in Computer Science, and possesses in-depth knowledge and understanding of network security violations (hacking). She is an expert of network security and has an in-depth understanding of the information security industry dynamics.

As President and Chief Executive Officer of Safety Net Canada, Ms. Smith brings the essential technical and business expertise, as well as the advanced people and managerial skills critical for the company's success. Furthermore, she has the vision and technological and business insight to lead the company to success.

Kathy Bronco-Vice President Corporate Development

As a co-founder of Safety Net Canada, Ms. Bronco brings superior skills and experience in customer service management and client relations. Ms. Bronco's background is in marketing and promotional initiatives. Safety Net Canada benefits highly from Ms. Bronco's superior organizational and people management skills.

Ms. Bronco has successfully planned and implemented advertising and media buying campaigns for a number of businesses in the British Columbia hospitality industry. Hotel Vancouver and the Executive Plaza Hotel are among the client accounts under her management and supervision.

As a Vice President of Corporate Development for Safety Net Canada, Ms. Bronco is responsible for managing and co-ordinating all advertising, promotional, and public relations activities. Her outstanding dedication, energy, and personal drive guarantee flawless execution of her role in the organization and make an excellent addition to the Safety Net Canada team.

Michael Adams-Vice President Business Development

Mr. Adams brings to Safety Net Canada more than 10 years of experience in the information technology and business development fields. He is an accomplished Senior Consultant and, for the past four years, has been the project manager for the implementation of an array of IT applications such as mySAP.com, SAP, BAAN, and DDC. Through these and other technology development and project management assignments, Mr. Adams has acquired valuable knowledge and experience in business process re-engineering and customer relationship management.

Before mySAP.com, Mr. Adams spent six years with Dynapro in the capacity of Senior Product Consultant. During his contract with Dynapro, Mr. Adams implemented an ERP system, was responsible for product materials management, and consulted senior management, vendors, and external stakeholders on business processes and project management deliverables.

Mr. Adams has an extensive technical and business education background. As the Vice President of Business Development for Safety Net Canada, he brings to the company exceptional organizational, logistics, and people skills essential to establishing a flawless and efficient business entity.

Shannon Aims-Vice President Distribution

Ms. Aims brings to the Safety Net Canada talent pool 10 years of experience in senior-level marketing and sales. She has worked as a Senior Account Manager for renowned Canadian and Australian corporations, including Honeywell International, BGE Service & Supply Ltd., and Nuchem Australia.

Ms. Aims is a multi-talented Sales and Marketing professional with a solid background of training and experience to support solution-based, business-to-business projects. She is highly skilled in evaluating operations and introducing efficiencies, as well as assessing the feasibility of product line innovations in relation to client-specific needs.

Ms. Aims' strengths are deeply rooted in efficient project management and superior service delivery, communication, and client relations (including management of high-profile accounts), innovation, and problem solving, as well as technology and business operations. She brings to Safety Net Canada the confidence, know-how, and determination necessary to successfully establish and manage client and partner relations.

Dean Martin-Investor Relations

Mr. Martin has more than 15 years of experience in the real estate industry and with global corporate and project financing. As a Vice President to Codwell Banker Commercial, he has been involved in corporate real estate investment projects valued in the tens of millions of dollars. Mr. Martin's affiliation with the real estate investment firm Century 21 has resulted in the successful completion of multiple company mergers and joint ventures in the area of commercial real estate acquisitions.

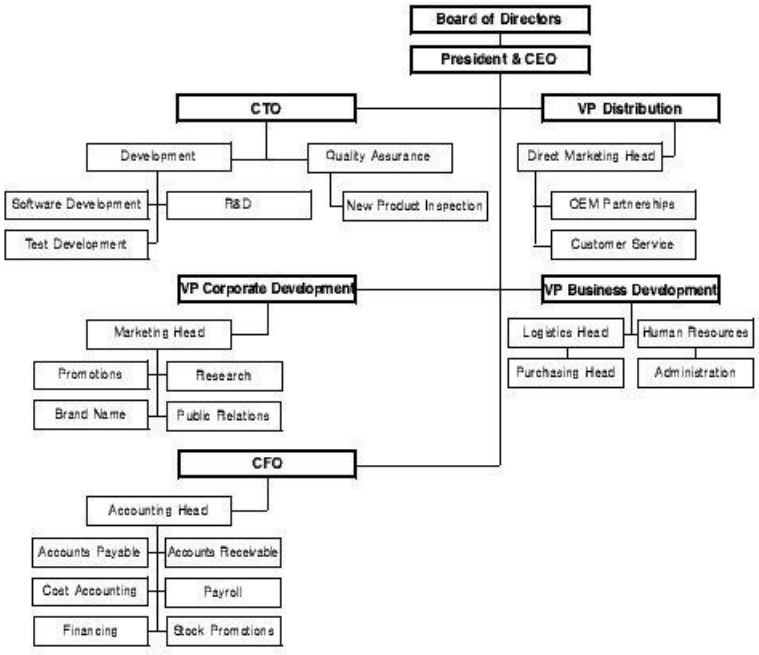
Mr. Martin has been actively involved in the funding and financial management of a variety of large real estate investment projects, including fundraising for an investment project in the cemetery industry-which raised $6 million dollars investment capital-and participation in "Burns Bog"-a project valued at $2 billion. Currently, Mr. Martin is actively working on several joint venture opportunities in the entertainment, recreation, and hospitality industry. His background is in business administration, marketing, and sales, and he is a member of the Master Medallion Club (top 1% of industry professionals).

Mr. Martin is a significant addition to the Safety Net Canada's management team, as his business development expertise and years of investment experience are invaluable assets to the company's financial division.

Organizational Support

Safety Net Canada is planning to rapidly build its management team and functional divisions to reflect revenue and organizational growth. The increase in staff will correspond to revenue growth.

Safety Net Canada, Inc. Organizational Chart



Strategic Alliances

Safety Net Canada plans to form strategic alliances with large hardware equipment manufacturers and software companies as part of its plan to pursue an expansionary corporate level strategy through vertical integration.

Hardware OEMs

Safety Net Canada will seek to enter into licensed manufacturing agreements with hardware equipment manufacturers for the production and bundling of security products. Large computer hardware and network equipment makers, such as IBM and Hewlett Packard, will be considered as potential strategic alliance targets. Under these licensing agreements, the company will benefit from expedited market penetration and access to a large and committed installed base.

Software Companies

Forming an alliance with leading software companies will benefit Safety Net Canada in two directions. Potential exchange of technological know-how will provide the company with the product and technology

infrastructure to deliver the finest Internet and network security solutions. Moreover, through this strategic alliance, Safety Net Canada will seek access to a robust and ubiquitous distribution system to reach retail customers. Safety Net Canada is currently in the process of evaluating potential strategic partnership opportunities with leaders in the anti-virus and firewall segment of the Internet and network security industry.

Outsourcing Partnerships

Safety Net Canada is a research and development company. Manufacturing, marketing, and other functions will be outsourced to third parties. The rationale behind the outsourcing decision is to focus on the company's core competencies-innovation and product development. Management considers that Safety Net Canada will benefit from outsourcing the following functions:

Advertising and Promotion

Safety Net Canada will examine prospective advertising agencies to outsource its marketing and promotion functions. Criteria in choosing a suitable advertising partner include:

- Global reach and resource sharing
- Client base and successful brands
- Experience managing hi-tech accounts

Web Development

A complete e-commerce enabled website is an integral part of Safety Net Canada's sales strategy through the direct channel. The company will contract out a web development team to build, implement, and maintain the e-commerce website. Key factors of choosing a web development outsourcing partner include uniqueness and functionality of the e-commerce technology and cost of development and maintenance.

Exit Strategy

Through its development of superior technology over existing network security solutions and by being first-to-market with a complete, off-the-shelf network security product, Safety Net Canada will explore the revenue potential to its full potential. If, as the company grows, a suitable bidder emerges, Safety Net Canada will consider the possibility of being acquired by a larger Internet and network security company.

PRODUCTS

Overview of Security Products

Network security is a multi-faceted technology field incorporating four different aspects of information security: Authentication, Administration and Audit, Access Control, and Encryption. The first two building blocks of information security-Authentication, Administration and Audit-are commonly conceptualized and referred to as the 3As of information security. Most companies involved in the network security industry manufacture products applicable to one of these four information security fields. Some of the currently available product groups and technologies, as well as their underlying functionalities are listed below. A more detailed description of these technologies is provided in the Exhibits section.

Available Technologies and Products

Authentication Products

Authentication tools manage user, host, and message verification. Primary authentication technologies include:

- Passwords
- Tokens
- Smart Cards
- Biometrics

Administration and Audit Products

Security administration and audit tools allow network managers to control and document which users get access to which resources. Principal components of security administration and audit are:

- Policy Management Services
- Database/File Management
- Auditing Software
- Virtual Private Networks (VPNs)

Access Control Product Group

Access control tools enable network managers to restrict access and filter the data traveling across the network. Chief data access technologies include:

- Firewalls (hardware appliances and software applications)
- Proxy servers
- Security Monitoring and Intrusion Detection Tools
- Gap Technology Devices

Encryption Product Group

Encryption and decryption technologies, such as Public/Private Key Infrastructure (PKI) and digital signatures, are used to guard data transmitted over the network. Within this product group, VPN, encryption enablers, and e-mail encryption are the key areas of product development.

Multi-Functionality Solutions

Most off-the-shelf security products address a single aspect of network security, which allows for vulnerabilities at one or more of the remaining three levels of information security. The trend toward increasing frequency and damage of security attacks has boosted demand for complete and bulletproof information security solutions. A number of industry players and individual security consultants have taken advantage of this opportunity by offering customized security solutions, addressing all four aspects of network security, at premium prices.

Stateful multilayer inspection firewalls filter packets at the network layer, determine whether session packets

are legitimate and evaluate contents of packets at the application layer. They allow direct connection between client and host, alleviating the problem caused by the lack of transparency of application level gateways. They rely on algorithms to recognize and process application layer data instead of running application-specific proxies. Stateful multilayer inspection firewalls offer a high level of security, good performance, and transparency to end-users. They are expensive, however, and due to their complexity are potentially less secure than simpler types of firewalls if not administered by highly competent personnel.

Safety Net Security Solutions

Dial-up Internet accounts, even with their changing IP (Internet Protocol) address are easy targets for hackers, especially with security breaches in browsers and operating systems being discovered all the time. Network access via an "always on" connection, such as cable modem or xDSL, is particularly vulnerable to malicious and unauthorized intrusion due to its static IP address. Safety Net Canada will be the first network security company to introduce an information security solution that meets all criteria for reliability, compatibility, ease-of-use, and scalability. The flagship product line is comprised of two components: the Security™, a hardware appliance that protects hardware from intruders, and the Security Guard™, complementary firewall and anti-virus software applications to protect the operating system and applications. By working in compliance and complementing each other, these two products amalgamate into a bulletproof network security solution that is resistant to currently known loopholes in security hardware appliances and software. Safety Net Canada is dedicated to continue innovating its products by incorporating new research and technology in information security into its existing and future products.

Security™

Introduction

The Safety Net Canada proprietary Security™ is a hardware security device, based on the Gap Technology principle (see Exhibits for detailed explanation of gap technology), that resides on the connection between a computer and a modem. It monitors the inbound and outbound transmission pattern between these two devices to determine activity levels. If the device detects inactivity or idle connection for a pre-set amount of time (set by the user), it physically disconnects the computer from the network. Once the user resumes networking (i.e., requests a page on the Internet by following a link on their currently open browser), the Security™ detects the user input and re-establishes the network connection through the modem to the networked server in order to fulfill the request. Since the Security™ is placed in front of previously installed firewalls, the physical disconnection prevents outside access to the firewall itself (and anything behind it). If an intruder cannot access the firewall, he/she cannot break it.

The Security™ provides complete protection to hardware unsecured by firewall. Moreover, it closes the hardware vulnerability gap of existing firewalls by breaking the network connection physically and seamlessly to the user.

Hardware Specifications

The Security™ is a hardware security device-a micro gateway component on the network connection. It consists of:

- Chasis
- AC Power Supply
- Circuit Board

- Activation Switch
- Input and Output (for data transfer wiring)
- LEDs

Functionality

The Security™ provides the following functions and customizable options:

- Automatic Activation
- Artificial Intelligence Infrastructure
- Adjustable Re-connection Timer
- Signal Recognition
- Stand Alone Micro Gateway
- Category 5, Modular and 75-ohm coaxial cable compatibility
- Fingerprint Technology Option
- Remote Access Option

Features

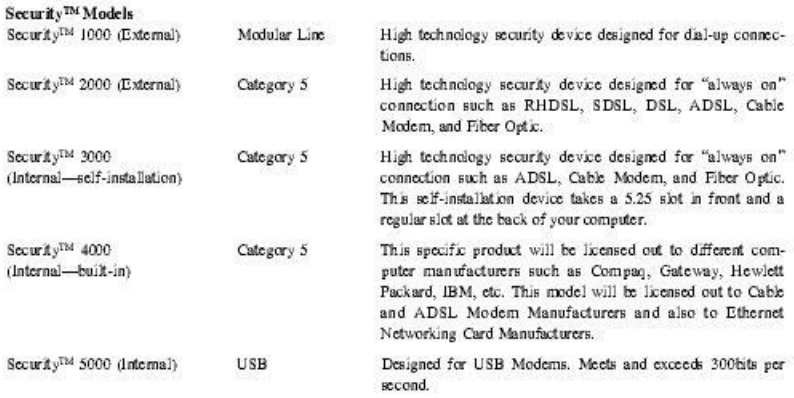
The above Security™ specifications and functionality encompass a number of considerable features:

- Security™ will protect:
  - Privacy of personal information and correspondence
  - Financial information
  - Medical records
  - Proprietary business information
  - All levels of users
- Security™ is compatible with all existing firewalls
- Security™ gives the user complete control of their networking (LAN) and Internet use
- Security™ provides the user with bulletproof privacy
- Security™ prevents unauthorized server access and information transfer without interfering with e-mail
- Security™ supports multiple connectivity infrastructures, including "always on" broadband, dial-up, wireless, and satellite-connected computers
- Artificial Intelligence Infrastructure provides for background functioning and seamlessness for the user. It notifies the user of browser inactivity and enables Automatic Activation within an adjustable time frame
- Security™ stops intruders from accessing the computer system, including hardware, software, and data
- Optional Fingerprint Technology protects the computer/network from local unauthorized access
- Easily customizable interface puts the user in control of activated security level
- Security™ monitors all inbound and outbound traffic to detect unauthorized intruders
- Optional Remote Access provides Security™ security functionality from virtually anywhere

Security™ Product Line

The Security™ product line supports both high-speed and dial-up connections, as well as wireless access. The different models comprising the company's Security™ product line are distinguished based on type of connectivity they support. Safety Net Canada will support every type of Internet and network connectivity-dial-up access and "always on" high-speed connections through high-speed modems, cable, and Ethernet cards, as well as wireless access. (The Security™ product mix is broken down by type of connectivity later on in the

plan.)



Security™ Models		
Security™ 1000 (External)	Modular Line	High technology security device designed for dial-up connections.
Security™ 2000 (External)	Category 5	High technology security device designed for "always on" connection such as RHDSL, SDSL, DSL, ADSL, Cable Modem, and Fiber Optic.
Security™ 3000 (Internal—self-installation)	Category 5	High technology security device designed for "always on" connection such as ADSL, Cable Modem, and Fiber Optic. This self-installation device takes a 5.25 slot in front and a regular slot at the back of your computer.
Security™ 4000 (Internal—built-in)	Category 5	This specific product will be licensed out to different computer manufacturers such as Compaq, Gateway, Hewlett Packard, IBM, etc. This model will be licensed out to Cable and ADSL Modem Manufacturers and also to Ethernet Networking Card Manufacturers.
Security™ 5000 (Internal)	USB	Designed for USB Modems. Meets and exceeds 300bits per second.

Security™ Models

Security™ Models

Security™ 1000 (External)	Modular Line	High technology security device designed for dial-up connections.
Security™ 2000 (External)	Category 5	High technology security device designed for "always on" connection such as RHDSL, SDSL, DSL, ADSL, Cable Modem, and Fiber Optic.
Security™ 3000 (Internal-self-installation)	Category 5	High technology security device designed for "always on" connection such as ADSL, Cable Modem, and Fiber Optic. This self-installation device takes a 5.25 slot in front and a regular slot at the back of your computer.
Security™ 4000 (Internal-built-in)	Category 5	This specific product will be licensed out to different computer manufacturers such as Compaq, Gateway, Hewlett Packard, IBM, etc. This model will be licensed out to Cable and ADSL Modem Manufacturers and also to Ethernet Networking Card Manufacturers.
Security™ 5000 (Internal)	USB	Designed for USB Modems. Meets and exceeds 300bits per second.

Security Guard™

The Security Guard™ is an anti-virus and firewall software program that complements the Security™ to create a comprehensive and unbreakable security solution for corporate networks and the home computer. The Security Guard™ will be bundled with Security™ devices that are sold through the industry distribution and re-seller networks. With the addition of these software applications, Safety Net Canada's Security™ becomes a reliable and seamless solution to the end-user security problem.

Accomplishments to Date

Initial design, prototype development, and testing of all hardware and software products in the Safety Net Canada flagship product line (Security™ 1000, 2000, 3000, and Security Guard™) have been completed. The company is currently involved in the final phase of design and testing of the final Security™ and Security Guard™ products. The projected release date for the Security™ line of products, including the Security Guard™ firewall and anti-virus software components, is scheduled to be available for distribution and sale by the end of Q1 2001. The e-commerce website and other marketing and sales strategies are under development and negotiations are underway to secure strategic partnerships with manufacturers and distributors.

Future Products

To maintain its leadership in the Internet and network security market, Safety Net Canada will continually improve its products and services in order to reflect and meet the needs of the dynamic and constantly changing hi-tech industry. Safety Net Canada's product mix will be an area of continuous multi-dimensional expansion, with new products developed in all four areas of network security and new technologies integrated into the existing product line.

Wireless Accessibility

Safety Net Canada has finished preliminary conceptualization of a wireless accessory to the Security™ device. Users of any Security™ desktop model will have the ability to communicate to their desktop (or corporate LAN) via a wireless access device. The wireless accessory will incorporate into a wireless access device (such as a cell phone or a handheld) seamlessly to the user.

Encryption and Access Control

Currently, research and development is focused on technologies in all four areas of network security, which can be successfully integrated with Safety Net Canada's existing product mix. Fingerprint authentication and encryption protection, as well as optical scanning technology are the fields of future development and product integration with Safety Net Canada's existing product line. Safety Net Canada is currently evaluating potential partnerships and product development opportunities with existing anti-virus software companies to expand the Security Guard™ component of its existing product line.

Satellite Scrambler Shield

Safety Net Canada plans to expand its Security™ product line to include a satellite scrambler shield device that protects satellite-connected computers from security vulnerabilities. Preliminary conceptual designs for the satellite scrambler shield are currently being generated.

Manufacturing

The manufacturing cost associated with producing the Security™ product line is competitive and low. This cost structure combined with the ownership of an exclusive patent-pending status provides for an optimal profit maximization environment for an extended period of time (14 years under the technology patent). Safety Net Canada is currently investigating potential manufacturers for the company's Security™ hardware devices. Criteria in selecting a suitable manufacturer include:

- Access to inputs at competitive prices
- Manufacturing capacity
- Delivery network
- Production time

Service and Support

Safety Net Canada will outsource the development of a highly secure, scalable, database-driven e-commerce website as part of its high-quality, streamlined Customer Relationship Management (CRM) program. The site will be capable of supporting high-volume sales and will provide 24/7/365 support for a worldwide customer base. All online sales will be fully integrated with the manufacturing and fulfillment processes for seamless

sales processing and inventory management.

Online Sales

Direct credit card sales of the complete Security™ line of products (bundled with the Security Guard™ firewall and anti-virus software) will be available to retail customers. Customers will have a choice of delivery options, such as delivery times and shipping methods. An international and reliable shipping company (such as FedEx) will be chosen to deliver Safety Net Canada's products to customers worldwide.

Product Registration

Through the website, customers will be able to register Safety Net Canada products upon purchase. Product registration will be the basis for customer tracking, support, and warranty service, as well as marketing.

Customer Support

Safety Net Canada Technology and Customer Support Center

This area of the website will be the central gateway for technical support to all customers of Safety Net Canada. It will provide account management support to corporate and retail customers. Implementation of single customer touch points will provide for superior long-term customer service. Unique customer IDs will be assigned to customers with registered Safety Net Canada products. The company will provide lifetime technical support to registered customers, with unique customers instantly identified through querying the customer database and seamless support provided via all means of communication (e.g. phone, e-mail, etc.).

General Support

This area will contain a product knowledge library, including FAQ, technical documentation and security issues and resolutions. In addition, the company's sales and support staff will receive general enquiries about Safety Net Canada products and additional product information (i.e., brochures). These requests will be processed via e-mail and potential clients recorded in the database. This area will also feature firmware configuration and installation instructions, as well as product updates and upgrades.

Warranty Service

A warranty service link will provide initiation of warranty service, generation of warranty tracking, and shipping instructions.

Intellectual Property

The company's Security™ technology process is protected by an exclusive patent-pending status that gives Safety Net Canada a worldwide advantage. The Security™ has an approved methodology patent pending in North America and a Patent Co-operation Treaty (PCT) applied. The PCT approval will provide the company with exclusive proprietary rights to the Security™ technology in more than 90 countries. Under these intellectual property agreements, no other business or entity can legally create or imitate the Security™ security device. Safety Net Canada maintains the privilege and power to sell manufacturing rights for a profit.

MARKET ANALYSIS

Global Need for Security

Vulnerability Factors and Risks

Internet Adoption

The *Computer Industry Almanac* predicts that the number of Internet users worldwide will grow to 766 million in 2005, more than double the online population in 2000. Internet adoption is largely saturated in North America, with the user base approaching 42% of the total North American population and 43% of the total online population worldwide. Most of the future growth of the Internet is predicted to take place overseas, with European users accounting for 30% and Asia-Pacific representing 25% of total worldwide users.

E-Commerce Growth

Increasing use of the Internet is beneficial to e-commerce and more businesses are migrating online to boost revenues and lower costs. While Internet adoption will grow overseas, e-commerce revenues will remain largely within the United States and amount to more than US $1.3 trillion worldwide by 2003. The business-to-business (B2B) sector is expected to contribute more than 85 percent of total global e-commerce revenue and add up to US $1.1 trillion in 2003. The business-to-consumer (B2C) sector will more than double and total US $178 billion in 2003.

In their Global Security Survey for 1999, PriceWaterhouseCoopers and *Information Week* report that e-commerce companies are one of the most vulnerable targets for security breaches. Compared to businesses that do not sell over the Internet, e-commerce companies are more pre-disposed to information and revenue loss as a result of security intrusions.

E-Commerce Firms at Higher Risk

Result of Security Breach	Firm Sells Online	No Online Sales
Information loss	22%	13%
Theft of data/trade secrets	12%	4%
Revenue loss	7%	1%

E-Commerce Firms at Higher Risk

E-Commerce Firms at Higher Risk

Result of Security Breach	Firm Sells Online	No Online Sales
Information loss	22%	13%
Theft of data/trade secrets	12%	4%
Revenue loss	7%	1%

Broadband Adoption

Broadband access is expected to become one of the most explosive segments of the online economy as Internet users are starting to prefer the faster and reliable cable and DSL services to the slower and inconsistent dial-up connections. Worldwide broadband access will grow to 70 million high-speed Internet subscribers by the end of 2003. Broadband access is expected to grow from 14 percent to 40 percent of total Internet connections.

Broadband connections not only provide increased bandwidth to users but also establish a 24-hour-a-day connection to the Internet. A Forrester Research survey of high-speed Internet subscribers confirms that constant connectivity and faster download are the top reasons for choosing broadband access. However, these

two features of high-speed Internet access expose users to the serious threat of security attacks. Constant connection and broader bandwidth increase the idle time for which a computer is connected to the Internet and, thus, open the door to intruder attacks.

Escalating Security Concerns

Explosive adoption of the Internet and e-commerce, as well as rapid commercialization of faster access technologies worldwide, have resulted in increased awareness of the importance of information security tools. Numerous instances of corporate security breaches have not only resulted in vulnerability to security attacks but also caused large monetary and reputation damages to renowned online businesses. As the frequency and magnitude of security attacks climbs, consumers become more concerned about invasion of their privacy and grow averse to shopping and conducting other transactions over the Internet.

Security Breaches

Globally, the number of companies reporting security breaches has surged from 53 percent in 1998 to 64 percent in 1999 (Source: *Information Week* Global Security Survey). Among the 2,700 executives and corporate security managers polled by the survey, 48 percent report hackers and terrorists as the probable cause of the breach (up from 14 percent in 1998) and 41 percent name authorized employees as the likely intruder.

Security Intrusion Costs

The fifth annual survey of computer crime and security, conducted by the FBI and the San Francisco-based Computer Security Institute, polled 640 corporations, banks, and government organizations about the state of their computer systems. Of the 90 percent reporting a security breach, only 42 percent could quantify the damage from the attacks. Nonetheless, the dollar figure losses as a result of security intrusion in 1999 are more than double the average annual total over the previous two years.

While information theft and financial fraud are causing the most severe financial losses, US $60 million and $58 million respectively, denial of service or server downtime, such as the ones that temporarily paralyzed Yahoo!, eBay, Buy.com, and several other websites in February 2000, are also a growing problem. The survey, which reports on numbers taken before the high-profile February strikes, quantifies the losses from denial of service attacks climbing from only US $77,000 in 1998 to US $8.2 million by the end of 1999. Loss of customers and public relations damage control are some of the intangible costs companies incur in association with security breaches.

Consumer Concerns

According to the 2000 American Express Global Internet Survey, which polled 11,410 Internet users and non-users across ten countries, four out of five people (79% of respondents) cited security and privacy issues as a concern when purchasing or making financial transactions online. A poll from Gallup and @Plan, taken shortly after the February denial of service attacks on major websites, reports that over 70 percent of online shoppers are concerned about privacy on the Internet in light of the attacks. The survey reveals that over 30 percent of online shoppers will be less likely to buy from e-commerce sites in the future and 85 percent of the respondents have privacy as their main concern regarding the Internet.

Security Market Overview

Industry Description and Size

The Internet and network security industry is a rapidly growing segment of the high-tech business sector, as businesses and individual consumers become more aware of the security threats caused by conducting transaction and exchanging information in a networked environment. Internet and network security is currently a US $5 billion business, growing two-fold from its 1998 level of US $2.3 billion. North America and Western Europe account for 84 percent of all 1999 network security sales, with North America at more than two thirds of total sales worldwide. Network security sales revenue is expected to grow even faster over the next three years, as Internet and broadband adoption, as well as e-commerce, continue expanding worldwide.

Growth Forecast

Security is not just for insurance purposes anymore but is an important part of corporate policy and strategy. The Internet is a source for increased profitability and companies need sophisticated security solutions to expand trusted relationships with their customers, partners, suppliers, and channels. This need is the vehicle of the network security market. According to IDC, its worldwide revenue will jump from less than $4 billion in 1999 to more than $11 billion in 2004.

IDC predicts that Authentication, Authorization, and Administration (3A) technology will be the leading sub-segments behind this industry growth. 3A technology is the largest segment of the network security industry and accounts for US $2.1 billion of total 1999 market revenues. IDC estimates that it will also be the fastest growing segment, at a compound annual growth rate (CAGR) of 28 percent from 1999 to 2004. The next nearest segments-firewall and anti-virus technologies-will each increase at CAGRs of 17 percent.

Safety Net Canada will take advantage of the vast profit and market share potential in the industry by being the first-to-market supplier of a complete network and Internet security solution to corporate and individual clients.

Industry Dynamics

There are more than 50 public companies operating in the network security industry. A growing industry and a large revenue potential indicate the presence of hundreds of other industry players-private companies involved in the development of new security technologies and products.

The industry is relatively fragmented and moving toward consolidation, as major players in the market are expanding into niche markets of the network security industry and rapidly gaining market share. Consolidation is expected to take two forms: research and development purchases for faster access to niche markets and diversification of revenue streams, and vertical integration through partnerships with software vendors (e.g., bundling with browsers and other software packages).

Regardless of consolidation trends, the network security industry will continue growing and attracting new participants within the next few years. The high revenue potential will provide for a competitive climate without an indication of market saturation in the short- to medium-term.

Distribution Channels

The network security industry has an established distribution network incorporating three main channels: distributors and re-sellers, licensing, and direct sales. Network security product manufacturers use these channels individually or in a combination depending on the product. Safety Net Canada intends to use an applicable combination of distribution channels for its network security products in order to reach a larger customer base and build market share.

Distributors and Re-sellers

Large computer components wholesalers, such as TechData (NASD:TECD) and Ingram Micro (NYSE:IM) are major distributors of network security hardware appliances and software products. These specific distributors deliver products to hundreds of thousands of resellers and reach customers in more than fifty countries worldwide. Safety Net Canada will investigate potential opportunities with a major computer components distributor in order to rapidly and efficiently rollout its products worldwide. Re-seller connectivity, global outreach and wholesale price will be among the top considerations in choosing a distributor.

Licensing

Licensing through Original Equipment Manufacturer (OEM) partnerships is a premiere distribution channel for security software products. Some hardware appliances are also licensed out and sold through network equipment manufacturers. Safety Net Canada will license its line of network security solutions to hardware and software manufacturers in order to reach the small business and home user market segments.

Direct Sales

Most manufacturers of network security products employ a full-service direct sales and support force to distribute their products, since a large portion of their revenue streams (in some cases up to 70%) is captured via support services. Direct sales channels usually comprise both an offline and an online channel, with most companies in the industry offering real-time 24/7/365 support and fully functional e-commerce websites.

Safety Net Canada will build an aggressive direct sales force in order to secure the enterprise target segment. The company will implement a complete total quality Customer Relationship Management (CRM) technical support program in order to build a loyal enterprise client base.

Target Markets

Safety Net Canada identifies the following four target market segments for its Security™ line of network security products.

1. Government and Non-Profit Organizations

Government agencies are a particularly lucrative market for the information security industry since they are major directories of highly sensitive information from personal data to military technology. A congressional subcommittee investigating the ability of federal agencies to protect computer systems from terrorists and hackers recently released a report card on government information security practices. Not one federal agency received an A, and the overall grade for the largest federal agencies and departments was D-minus. In response to these facts, the current administration is seeking $2 billion for information security in next year's budget, a 15 percent increase.

The Government is one of the largest spenders in the economy and Safety Net Canada will take advantage of the opportunity presented by detected vulnerabilities of government information systems. The company will aggressively market its budget-conscious Security™ security solution to all levels of government administration and non-profit organizations in order to capitalize on this vast revenue opportunity.

2. Large Corporations

Enterprise customers are a high priority target market for the network security industry since a substantial volume of sensitive information and e-commerce transactions is exchanged over corporate networks and the Internet daily. Large corporations over 10,000 employees are expected to be top network security spenders, with security budgets increasing proportionately to company sizes.

Safety Net Canada will respond to the growing needs for security of larger corporations by providing a complete security solution, resistant to hacker attacks and internal security breaches.

3. Small and Medium Enterprises (SMEs)

SMEs are the primary market for cost-efficient high-speed Internet access. Growing broadband adoption among SMEs indicates increased vulnerability to security attacks of this market segment. As businesses become more exposed to networking and the Internet, they become a substantial target market for the network and Internet security industry.

U.S. Business Broadband Users 1999-2003 (Millions)

	1999	2000	2001	2002	2003
Fiber	1.71	2.36	3.15	4.07	5.07
DSL	0.15	0.42	0.73	0.93	1.1
Cable	NA	NA	NA	NA	NA
Satellite	NA	NA	0.02	0.04	0.25
Wireless	0.04	0.15	0.57	1.59	3.09
Copper T-1	1.6	1.9	2	1.9	1.8
Total	**3.49**	**4.83**	**6.47**	**8.53**	**11.3**

U.S. Business Broadband Users 1999-2003 (Millions)

U.S. Business Broadband Users 1999-2003 (Millions)

	1999	2000	2001	2002	2003
Fiber	1.71	2.36	3.15	4.07	5.07
DSL	0.15	0.42	0.73	0.93	1.1
Cable	NA	NA	NA	NA	NA
Satellite	NA	NA	0.02	0.04	0.25
Wireless	0.04	0.15	0.57	1.59	3.09
Copper T-1	1.6	1.9	2	1.9	1.8
Total	**3.49**	**4.83**	**6.47**	**8.53**	**11.3**

Safety Net Canada will target SMEs by offering "easy to install and use" and complete network security products at reasonable prices.

4. Individual Home Computing

Broadband adoption among home users will grow even faster than business users, with residential subscribers reaching 20.73 million across all broadband channels.

U.S. Residential Broadband Users 1999-2003 (Millions)

	1999	2000	2001	2002	2003
Fiber	0.05	0.1	0.17	0.24	0.32
DSL	0.39	1.42	3.35	5.69	9.85
Cable	1.47	2.94	4.99	7.27	9.78
Satellite	NA	NA	NA	NA	NA
Wireless	0.02	0.08	0.24	0.53	0.77
Copper T-1	NA	NA	NA	NA	NA
Total	**1.94**	**4.54**	**8.75**	**13.73**	**20.73**

U.S. Residential Broadband Users 1999-2003 (Millions)
U.S. Residential Broadband Users 1999-2003 (Millions)

	1999	2000	2001	2002	2003
Fiber	0.05	0.1	0.17	0.24	0.32
DSL	0.39	1.42	3.35	5.69	9.85
Cable	1.47	2.94	4.99	7.27	9.78
Satellite	NA	NA	NA	NA	NA
Wireless	0.02	0.08	0.24	0.53	0.77
Copper T-1	NA	NA	NA	NA	NA
Total	**1.94**	**4.54**	**8.75**	**13.73**	**20.73**

Another trend in residential Internet access is the development and commercialization of home-based local area networks (LANs). The growth of home LANs is being driven both by multi-PC households and by high-speed Internet access. By 2004, 67.7 million American homes (63.4%) will have PCs, with 30.4 million of these housing more than one. Of the multi-PC households, 58 percent will be networking their devices by 2004.

Increased residential broadband access and a growing number of home-based LANs create a substantial security threat to home users. Safety Net Canada intends to aggressively target this segment in order to secure market share and realize the revenue potential offered by the home user market.

Buyer Trends

International Broadband Adoption

Western Europe will mirror the U.S. broadband industry development, with European high-speed Internet subscribers reaching 18 percent of households (or 27 million) from a minute 0.2 percent of households in 1999. Scandinavia and the Netherlands, with their traditionally high penetration rates, will take the lead with Germany and the United Kingdom following closely.

Another booming region for the broadband industry is Asia-Pacific. The number of broadband subscribers in the Asia-Pacific region is predicted to surge from 452,900 at year-end 1999 to 11.3 million by the end of 2003. Cable modem and ASDL will be the most popular forms of access, taking 46 percent and 42 percent of the market respectively by year-end 2003. Competing broadband providers across the region are focusing on SMEs and home offices as an entry strategy into this market. Further commercialization of broadband services will lead to increased competition, as international companies, such as Global Crossing and Level 3, have launched their services into the market.

Preferences for Security Solutions

Corporations would like to have one network security package that solves all of their security needs including:

Products that employ all 4 areas of network security:

- User ID/Authentication
- Encryption
- Access Control and Privilege Management
- Administration and Audit

Products that meet the following criteria:

- Ease-of-use
- Interoperability
- Scalability
- Ease of administration
- Integration with existing customer applications
- System reliability and availability

Strategic Opportunities

The complexity of competing information and network solutions-both software and hardware-based-provides a significant opportunity to the company in marketing its complete, off-the-shelf, user-friendly network security solution. Safety Net Canada's Security™/Security Guard™ product line provides a high-level of reliability and matches client requirements for compatibility and ease-of-use.

Safety Net Canada will be the first mover in providing an all-inclusive security solution, incorporating all four segments of the network and Internet security industry. The current level of dial-up accessibility (more than 80% of Internet subscribers in 2000) will allow for quick market penetration of the Security™ 1000 model and rapidly growing market share and revenue for Safety Net Canada. Beneficial broadband adoption trends will ensure success for the company's Security™ 2000 and 3000 models, with market share and revenue increasing in parallel to the popularization of high-speed access.

Environmental Issues

Trends in most exogenous market variables, applicable to Safety Net Canada's business model, will have a positive impact on the company. Technology developments, social attitudes, and regulation are the external market factors that will potentially influence the development and success of Safety Net Canada.

Technology Development

The hi-tech industry is subject to constant fluctuations, as the life cycle of technology is short and it becomes obsolete every 18 months. Safety Net Canada welcomes the challenges of rapidly evolving technology and, through utilizing its strategic partners and internal team of tech-savvy and innovative individuals, the company

will become a trendsetter for new technology adoption and implementation.

Social Attitudes toward Security

As more people become connected through computer networks and the Internet, security concerns are inevitably on the rise. This would only benefit the company in the long term, as the team of Safety Net Canada is dedicated to continue innovating and bringing the best security products and services to the wired (and wireless) population.

Regulatory Issues

Strictly enforced information security standards could become an obstacle for vendors of software applications (firewall and anti-virus software). For Safety Net Canada, such standards would only encourage sales of the Security™ product line, since it is highly reliable and independent of any hardware and/or software platform.

MARKETING PLAN

Marketing Objectives

Building a strong corporate and retail customer base and developing a high industry image and profile are corporate-level objectives subject to the company's marketing and promotional efforts. Each of these goals will be pursued and achieved through the implementation of an array of marketing and promotional actions geared towards fulfilling the directives of Safety Net Canada's marketing plan.

Build Customer Base

Building a loyal customer base of corporate and retail clients involves implementation of the following strategic marketing actions:

- Implement an effective and competitive product mix strategy to successfully position the Security™ product line as the leading Internet and network security solution on the market.
- Development of an e-commerce website with well-documented and displayed inventory and effective, efficient, and hassle-free retail and corporate service and support.
- Aggressive advertising in print and electronic media to create brand awareness and educate the public of the risks associated with broadband access and incomplete corporate security solutions.
- Sales strategies implementation including reseller networks, affiliate programs, corporate sales development, and direct marketing campaigns (including co-marketing).
- Exhibiting at business and computer industry conferences and trade shows and high-visibility consumer home and computer shows.

Develop a High Industry Profile

The company recognizes the importance of developing and maintaining a prominent place and a positive image in the Internet and network security community in order to sustain credibility, attract the highest quality of strategic partnerships and alliances, and position the company for successful execution of its exit strategy. Safety Net Canada's brand and image will positively benefit from:

- Publicity through news releases and announcements
- Participation in industry trade shows
- Membership and active participation in industry associations, initiatives, and studies

Security Marketing Mix

The Security™ marketing mix features competitive pricing, mass customized packaging, and creative distribution and promotional tactics to guarantee target market reach and revenue growth.

Flagship Product Line

The Security™ flagship product line comprises the Security™ 1000, 2000, and 3000 models, complemented by the Security Guard™ software. These three models meet the security needs of an established (dial-up) and a growing (broadband) market, which will allow Safety Net Canada to acquire market share in the current market and grow its market presence in the future.

Product Pricing

The Security™ product line is competitively priced at US $110 at the retail level. Distributor price is set at US $45.

Product Packaging

Safety Net Canada will employ separate product packaging strategies for its two general groups of customers:

- **Corporate Users** -Default packaging for corporate users will exclude the Security Guard™ from the product bundle. The rationale behind this is that most corporate users have already installed firewall and anti-virus software solutions on their corporate network. The Security™ can match corporate users' requirement for compatibility by seamlessly integrating into existing security software applications.
- **Small Business and Home Users** -A large number of home and small business users do not have anti-virus and firewall applications on their computers. Therefore, small business and home users will be provided with the Security™ device and the Security Guard™ as a bundled package. This form of packaging offers to the target customer group of home and small business users a unified, plug-and-play security solution that solves all incompatibility and vulnerability problems.

Product Sales Strategy

Safety Net Canada will incorporate a combination of distribution channels in order to pursue an aggressive and effective product sales strategy. Safety Net Canada considers the integration of direct sales and industry distribution as the fastest and most cost-efficient approach to penetrating the Internet and network security market. In order to generate superior sales results and meet unit and dollar sales targets, Safety Net Canada will provide special sales training programs to intermediaries and sales incentives to the direct sales force.

Industry Distribution Channel-70%

Safety Net Canada will gain access to a robust worldwide distribution network via partnering with international distributor of computer components. Prices to intermediaries afford them reasonable profits that will encourage intermediary flexibility. The Security™ 1000 and 2000 external devices, supplemented with the Security Guard™ software applications will be distributed primarily through this channel. Through the OEM manufacturing license agreements, Safety Net Canada will gain access to the international distribution network of a large hardware manufacturer. This industry distribution channel is best suited for the Security™ 3000 internal device with the corresponding version of the Security Guard™.

Direct Sales-30%

Direct sales will account for 30 percent of total Security™ sales and will be administered through the e-commerce website and by the Safety Net Canada direct sales force. The direct sales channel will accommodate management of most corporate accounts and large corporation purchases. All three flagship models of the Security™ device will be sold directly, with the option of adding the Security Guard™ software.

Advertising and Promotion

Safety Net Canada will utilize an abundant assortment of online and offline advertising and promotion tactics to build a solid global brand name and establish a high corporate profile in the technology industry.

Online Marketing

A comprehensive and consistent online marketing campaign is crucial to any company in the technology sector. Creating a robust, multi-functional, easy-to-use, and appealing website is a vital component of a successful online marketing program. Driving traffic to the website and closing the sale online are fundamental to securing the corresponding revenue stream.

Safety Net Canada E-Commerce website

The company will contract a team of professional web developers to build its e-commerce website. Anticipated features and components of the site include:

- Product presentations and technical information
- Library of knowledge on Internet and network security, including latest industry and technology news
- Multi-level technical support 24/7/365, with password-protected areas for large clients, partners, and affiliates
- Fully-functional e-commerce and inventory control back-end, supporting worldwide demand for Safety Net Canada products

Driving Traffic

This will be accomplished by a variety of online marketing tactics, with a portion of the advertising budget allocated but not limited to:

- **Search Engine Registration** -The company will register with top search engines using selected keywords (meta tags), such as security, anti-virus, firewall, etc.
- **Banners and Buttons** -The company will investigate link and banner exchange options compatible with Safety Net Canada. In addition to affiliate website advertisements, button and banner ads will be placed on selected hardware, network security, and other industry-related websites.
- **E-zines** -The targeting capabilities of e-mail newsletters, or e-zines, transform this into one of the best marketing tools that the Internet offers. The newsletter for Safety Net Canada will notify registered members of new and upcoming product updates and upgrades and keep in touch with the opt-in client community. Safety Net Canada will be featured in the top independent e-zines currently on the Internet. The company will feature in e-zines geared towards MIS and IT managers and corporate network professionals.
- **E-mail Marketing** -The success rate of opt-in e-mail broadcasts is approximately 17 percent (quite

high for any form of direct marketing). The purchase or acquisition of targeted consumer lists, as well as targeted e-mail harvesting, will be used to source out prospects in lieu of Safety Net Canada's direct sales strategy. The company will use only targeted lists and e-mails to eliminate spam.

Offline Promotion

Complementary to its online marketing program, Safety Net Canada will employ a number of offline advertising and promotional actions to publicize the brand name, attract re-sellers, and reach customers. Safety Net Canada will promote itself through the following specific offline media:

Trade Shows

Safety Net Canada will lease exhibition space at some of the largest and most popular hi-tech industry trade show events. The following annual, nationwide hi-tech, and information security events will be considered as potential venues: Comdex, InfoSec World, and Annual Computer Security Conference and Exhibition (Computer Security Institute). These specific trade shows attract a large number of information security exhibitors, as well as a mass of wholesale and retail customers.

Print Publications

Much like e-zines, offline magazines dedicated to information security will be carefully chosen to promote Safety Net Canada. The rationale is that online and offline media combined reach a larger customer base than each medium separately.

Public Relations

A successful public relations campaign requires a close partnership with the media. Safety Net Canada will seek allies among publishers and columnists and will use website reviews and news releases as vital promotional techniques. Promotional channels to be considered include technology television and radio shows, publications for IT professionals, etc.

Target Market Penetration

The Security™/Security Guard™ product line will be rolled out into all four target market segments simultaneously. Different blends of distribution channels and marketing techniques will be used to reach the various market segments.

Large Organizations

This target segment encompasses large corporations, government agencies, and non-profit organizations. Safety Net Canada will market to this target segment through both the distribution network and direct sales channel. Trade events and online corporate account management will be the tools for reaching this market.

Small Business Customers

Small businesses are the fastest organizational units adopting broadband Internet access. The need for high-speed access echoes a need for better security solutions and Safety Net Canada will match this requirement by

reaching small enterprises primarily via the industry distribution network. Print publications, trade shows, and opt-in e-mails are among the techniques the company will use to market its products to small businesses.

Home Users

Strategic banner advertising and advertising through distribution intermediaries will be used to attract home users. Home users will be provided with an off-the-shelf, easy-to-install and use, and complete security solution. Safety Net Canada products will be sold to home users predominantly through the intermediary distribution networks.

Global Rollout Strategy

Safety Net Canada will build its market share by gradually entering all major international markets by the end of the planning period subject to this plan. While all products will be available worldwide through the Safety Net Canada website, initial marketing and reseller network building will be focused on North America. The United States and Canada will be the opening markets for the Security™/Security Guard™ product line. Within six months of North American market entry, the company will move quickly towards entering Asia. Hong Kong will be the entry point for China and Asia overall, with the Korean, Taiwanese, and Japanese markets penetrated by the end of year two. Initial entry into Europe will also commence in year two, with the United Kingdom being the entry point. By the end of year three, Safety Net Canada expects to have a substantial market share in all of North America, Asia, Europe, and Latin America.

COMPETITION

Competitive Climate

As the Internet and network security industry is projected to grow, the competitive environment will become more heated. Competition will ensue from both incumbent companies and new entrants. Established technologies, such as firewall software, will be subject to downward price pressure and low-cost competition. The competitive rules for newer information security technologies, such as Gap technology appliances, will continue to be derived from product innovation rivalry and differentiation.

Direct Competition

Safety Net Canada has no close direct competitors for its complete Security™/Security Guard™ security solution. None of the company's industry rivals offers a software- and hardware-integrated, off-the-shelf, and easy-to-use security product.

Indirect Competition

There are indirect competitors to individual components of Safety Net Canada's product line. Indirect competitors are classified according to type of security product and described below. Safety Net Canada's differentiators are explained after each competitor classification group.

Gap Technology Devices

Gap technology allows for a physical "disconnection" between two logically connected networks. The physical disconnection prevents security intrusion while the logical connection allows the two networks to share

resources. (A discussion on Gap Technology is located in the Exhibits). Most Gap Technology devices are designed for protection of the internal corporate network. The key players in this industry segment are described below.

Market Central Switch

Switch is the core product in Market Central's suite of security offerings. It is a network switcher in its most straightforward implementation. It is designed similar to the common keyboard/video/mouse (KVM) switches, except that it deals exclusively with network connections.

Switch has two knobs on the front connected by a crossbar that forces them to be turned simultaneously. The rear of the switch has four Ethernet outlets, two for each network the user wishes to connect to. The host PC must have two network interfaces to allow it to connect to the two networks. The network cables from the PC's interfaces are connected to the network interface card (NIC) ports on the switch, leaving the other two connections for the individual LAN cables. The network cards should be attached to the same side of the switch as their corresponding LAN cables, to ensure that there is no accidental crossover. Once the four cables are attached correctly, the user must turn either knob to switch from network "A" to network "B" (hence the crossbar). The flagship SecureSwitch™ costs US $399 to the consumer.

Beyond the basic network-switching model, the user can upgrade Switch to include keyboard/video/mouse-switching capabilities for a fee. In this case, all services switch at once. This allows the use of two workstations with a single keyboard, monitor, and mouse. When one system is active (and on the network), the other is not. The retail price of the Switch is US $528.

The next step up is the Switch Information Security System, which is designed to limit and log access to restricted systems. It does this via a hardware token, which must be presented before network connectivity or AC power is enabled on the PC. This allows administrators to grant access to a system while limiting some users to "offline" work if network privileges are not included.

Exhibits

Market Central also sells Data Bolts (US $59), simple and inexpensive switches meant to disconnect your local LAN when you connect to the Internet.

Differentiator: While Market Central's Switch allows for physical disconnection between desktop and network or two networks, it requires manual intervention from the user every time the connection needs to be broken or re-established. Safety Net Canada's Security™ is seamless to the user and is more cost-effective compared to Switch, retailing at $110 and $399 respectively.

RVT Stop-IT®

RVT Technologies is a Lilburn, Georgia, based company producing the Stop-IT® Internet and network security solution. The Stop-IT® product line functions on the principles of gap technology and currently consists of two form factors: one is an internal PC card and the second is an external device that is situated in front of the modem. Both devices intercept incoming network traffic

before it reaches the personal computer and monitor it based on an internally stored signature.

The target market for Stop-IT® is ADSL and cable modem users, who are continuously connected to the Internet. Stop-IT® is a single-user device, and employs an upgradeable EPROM to store its virus signature library. It makes use of an optical isolator to introduce the air gap as required. Any information that is sent to the PC must pass through the device, where it is scanned before it reaches the system. If any of the data matches any virus signature, the light signal is cut, and the data is dropped. The signal is automatically resumed once the identified threat ends, causing minimal disruption to the end user.

Differentiator: Although within the price range of the Security™ models, RVT Stop-IT® is essentially a sophisticated virus filtering hardware card. RVT Technologies has scheduled product launch for the Stop-IT® line to commence in January 2001. The Stop-IT® product line will not offer the high level of protection of Safety Net Canada's Security™ line.

Whale Communications

Whale Communications is a privately-held New Jersey company that manufactures Shuttle-a hardware device that is placed between two endpoint servers, creating an air gap. The servers are on different networks that are not otherwise connected. Each server is configured to be the gateway from its network to the other, funneling all inter-network traffic through the gap. Shuttle is a non-programmable unit consisting of an analog switch and a SCSI-based memory bank. The switch is designed to connect to one or the other host, but never both. It uses short-circuit detection to ensure that it is functioning as designed. The function is to connect to one network, read any awaiting information, switch over, and push the data onto the second network. It alternates between the networks at speeds that allow a theoretical transfer rate of 130 Mbps. The system is comprised of the appliance and two PC hosts-one external and one internal.

Differentiator: Although Whale Communications claims that the system provides bulletproof security, it does not protect against denial-of-service attacks, configuration errors, internal attacks, or fraudulent transactions. It must be used in conjunction with other measures (such as firewalls and internal access authorization policies) in order to provide 100 percent security. The cost is US $43,000.

SpearHead Technologies Ltd.

Privately-held, SpearHead Technologies Ltd. is an Israel-based network security company manufacturing and distributing the AirGAP hardware device. Similar to AirGAP is a hardware network appliance that shuttles data between two mutually exclusive connections. However, whereas e-Gap™ is designed to connect (or disconnect) two machines, AirGAP is meant to connect two full-scale networks.

The AirGAP solution is a combination of hardware and software that comes in three models: AG100, AG200, and AG300. The hardware component contains three controllers: a master, a slave, and a content-inspection board. The gap lies between the slave and the content-inspection board,

and there is no live session between the two networks at any given time.

With a hardware speed of 800 Mbps, the AG300 can sustain an average user base of about 5,000 to 10,000 (or about 1,000 concurrent sessions). The AG100 can handle smaller workgroups of approximately 1,000 users.

Differentiator: While AirGap security appliances can protect stand-alone personal computers, they are too expensive to appeal to the general consumer market. Safety Net Canada will target the corporate market segment by providing an exceptionally cost-effective and bulletproof corporate PC security solution.

Hardware Firewall Appliances

Hardware firewalls are the predecessor Gap Technology devices. There are two key players in the hardware security appliances industry segment, with their products geared towards different buyer segments.

WatchGuard Technologies Firebox

Founded in 1996, WatchGuard Technologies produces the Firebox-a hardware based network security appliance. The Firebox product line caters to corporate users including small business and large corporations. WatchGuard's enterprise products start at $4,990 to a high of $12,990. For the SOHO user (small office/home office), the base cost of WatchGuard (10 users) is $449 to a high of $1,000 for 50 users and an additional $449 to include the virtual private network (VPN) option. Other products include the WatchGuard VPN Manager at $995 for up to 4 Fireboxes to $7,005 for unlimited Fireboxes.

Cisco Secure PIX Firewall

The Cisco Secure PIX Firewall is the dedicated firewall appliance in Cisco's firewall family and holds the top ranking in both market share and performance. The Cisco Secure PIX Firewall delivers strong security and creates little to no network performance impact. The product line enforces secure access between an internal network and Internet, extranet, or intranet links. The Cisco Secure PIX Firewall scales to meet a range of customer requirements and network sizes and currently consists of four models:

1. The new Cisco Secure PIX 525 is the latest and largest addition to the PIX 500 series and is intended for Enterprise and Service Provider use. It has a throughput of 370 Mbps with the ability to handle as many as 280,000 simultaneous sessions. The 600 MHz CPU of the PIX 525 can enable it to deliver an additional 25-30 percent increase capacity for firewall services.
2. Cisco Secure PIX 520 is intended for large enterprise organizations and complex, high-end traffic environments. It also has a throughput of up to 370 Mbps with the ability to handle 250,000 simultaneous sessions.
3. Cisco Secure PIX 515 is intended for Small/Medium Businesses and remote office deployments and has throughput measured at 120 Mbps with the ability to handle up to 125,000 simultaneous sessions.
4. Cisco Secure PIX 506 is intended for high-end Small Office/Home Office organizations and has throughput measured at 10 Mbps (3DES of 7 Mbps).

All four Cisco Secure PIX Firewall models have IPSEC encryption built-in, permitting both site-to-

site and remote access VPN deployments, and operate on a hardened operating system focused on protecting both the security of the device and the networks it protects. In addition to having the ability to be managed by the PIX Configuration Manager, the Cisco Secure PIX Firewalls also may be centrally managed by the Cisco Secure Policy Manager, which can manage up to 500 PIX Firewalls, Cisco Secure Integrated Software deployments, and site-to-site VPN installations.

As a dedicated appliance, the Cisco Secure PIX Firewall is easy to install and stable. The average price for this product line is approximately US $8,000.

Differentiator: Hardware firewall appliance manufacturers are not outfitted to respond to the needs of the small business/individual user. These are expensive server protection devices that are targeted at large corporate networks. Safety Net Canada will protect the desktop within the corporate network.

Firewall and Anti-Virus Software

The firewall and anti-virus software segment of the industry is highly competitive. There are more than 50 public and hundreds more private companies producing information security software. The top four players (all of them are public enterprises) and their security products are described below.

Symantec Norton Anti-Virus and Firewall Software

Symantec is a Cupertino, California, based company with 2,600 employees worldwide. Symantec is the producer of the extensive Norton line of security products. The product mix includes an enterprise, a small business, and a home-user solution. The software has four main functions:

1. **Virus Protection** -Symantec's anti-virus solutions protect computers and networks at multiple entry points from known and unknown threats.
2. **Mobile Code Protection** -Symantec's mobile code solutions protect customers from the malicious attack by legitimate technologies such as Java applets, Active X controls, auto-executable plug-ins and push-clients which can be used to deny service to customers, modify data, steal passwords and files, or even redirect modem dial-ins without a user being aware they are running a program.
3. **E-Mail Content Filtering** -Symantec's e-mail content scanning and filtering solutions help protect proprietary information, reduces liability exposure, and improves productivity for e-mail applications.
4. **Internet Content Filtering** -Symantec's Internet content filtering and management allows individuals and organizations to control and focus Internet usage for increased productivity and decreased liability.

Network Associates McAfee VirusScan

Suitable for individual users, small businesses, and large companies, McAfee VirusScan is a virus detection and removal solution for a major source of infection: the desktop machine. VirusScan has a broad platform coverage (PC, Mac, Unix, and Wireless) and fits seamlessly into any networked environment, with a wide array of proactive manageability and visibility features, ensuring an effective virus security solution for users.

Check Point Software

Check Point Software, an Israel-headquartered developer of security software, produces FireWall-1-an enterprise firewall solution for large organizations.

The FireWall Module is deployed on Internet gateways and other network access points. The Management Server downloads the Security Policy to the FireWall Module, which protects the network. The FireWall Module can be installed on a broad range of operating system platforms (Windows NT, Solaris, HP-UX, and IBM AIX). The FireWall Module includes the Inspection Module and the FireWall-1 Security Servers. The Security Servers provide the following authentication and content security features:

- **Authentication** -The Security Servers provide authentication for users of FTP, HTTP, TELNET, and RLOGIN. If the Security Policy specifies authentication for any of these services, the Inspection Module diverts the connection to the appropriate Security Server. The Security Server performs the required authentication. If the authentication is successful, the connection proceeds to the target server.
- **Content Security** -Content Security is available for HTTP, FTP, and SMTP. The HTTP Security Server provides content security based on schemes (HTTP, FTP, GOPHER, etc.), methods (GET, POST, etc.), hosts (for example, "*.com"), paths, and queries. A file containing a list of IP addresses and paths to which access will be denied or allowed can be used. The FTP Security Server provides content security based on FTP commands (PUT/GET), file name restrictions, and anti-virus checking for files transferred. The SMTP Security Server provides content security based on "From" and "To" fields in the mail envelope and header and attachment types. In addition, it provides a secure send mail application that prevents direct online connection attacks. The SMTP Security Server also serves as an SMTP address translator, that is, it can hide real user names from the outside world by rewriting the "From" field, while maintaining connectivity by restoring the correct addresses in the response.

Differentiator: Unless used with additional devices and security monitoring, firewall and anti-virus software (although inexpensive) is insufficient in preventing security breaches from outside. Moreover, none of the existing security software applications can prevent insider security breaches-a major concern for organizations online. Safety Net Canada combines a hardware and software component to offer organizational and individual users an off-the-shelf, competitively priced product impervious to both insider and outsider attacks.

Competitive Advantage

Safety Net Canada's competitive advantage is two-dimensional. One aspect of it is the company's ability to differentiate its products, based on core competencies-innovation in product development and superior customer service. The second source of competitive advantage is cost-efficiency, with Safety Net Canada being the sole player in the Internet and network industry able to deliver a multi-faceted reliable security solution at nominal cost. Long-term sustainability will be achieved through continuous innovation and customer service improvement.

Barriers to Entry

Safety Net Canada intends to lock out competitors via employing the exclusive manufacturing rights to the Security™ technology worldwide. Utilizing alliances with large hardware OEMs will allow for rapid market

penetration and raise the barriers for new entrants in the industry.

FINANCE

Revenue Streams

The revenue model of Safety Net Canada comprises a primary and a secondary revenue category, with each category containing multiple revenue streams.

Sales through Distributors

Revenue derived from distribution network sales contributes up to 70% of total revenue and is composed of:

- Security™ 1000 Sales-26% of distribution network revenue and 13.4% of total revenue from all channels
- Security™ 2000 Sales-35% of distribution network revenue and 20.3% of total revenue from al channels
- Security™ 3000 Sales-39% of distribution network revenue and 35.6% of total revenue from all channels

Direct Sales

Revenue derived through the direct sales channel comprises approximately 30% of total revenue and consists of:

- Security™ 1000 Sales-26% of direct sales revenue and 7.9% of total revenue from all channels
- Security™ 2000 Sales-35% of direct sales revenue and 10.9% of total revenue from all channels
- Security™ 3000 Sales-39% of direct sales revenue and 11.9% of total revenue from all channels

EXHIBITS

Information Security Products

Authentication Products

Authentication tools manage user, host, and message verification. Primary authentication technologies include:

Passwords

Most operating systems and software applications have built-in password functionality. Passwords can limit access and protect hardware devices (such as hard drives and printers), user accounts, files, corporate network data, etc. The disadvantage of passwords is that they can be deciphered or stolen if made available to outsiders.

Tokens

Tokens are computer-generated authentication tools (such as numeric or alphanumeric keys) that authorize access for the computer, as opposed to the individual. A considerable fault of tokens is their inability to protect the individual from internal security attacks (as in corporate scenarios).

Smart Cards

Smart cards are physical plastic cards that carry original information, such as a unique number or a unique combination of data about their owner. Similar to credit cards, smart cards allow for seamless purchasing transactions and are applicable to online shopping as a shopper authentication tool. The drawbacks of smart cards are that they are easy to lose, inconvenient to carry, and require additional investment in smart card reading hardware devices.

Biometrics

All individuals are unique and this is what biometrics authentication technologies rely on to identify unique users. Fingerprint, voice, and retina scans are the currently available methods of differentiating individuals. These authentication technologies are implemented in two stages. First, a user needs to register his biometric information into the authentication system. This involves scanning and creating an image of a person's fingerprints or eye retina, or recording a sample of a person's voice. Associated with these samples are the user ID and other information. During authentication, the user's fingerprint is scanned or his/her voice recorded into the system and compared to the sample stored in the database. The matching result, by minutiae or template pattern comparison, confirms if the user is pre-registered or not.

Biometrics authentication is not yet widely commercialized but its numerous industrial applications are an indicator of future for this technology.

Administration and Audit Products

Security™ administration and audit tools allow network managers to control and document which users get access to which resources. Principal components of security administration and audit are:

- **Policy Management Services** -These are applicable primarily to the corporate environment and involve: devising of security strategy, security implementation procedures, hiring of qualified network security professionals, etc. These services provide for the generation of custom-tailored security solutions and are effective in combating security crimes. The disadvantage of these services is that they are usually expensive and beyond the purchasing capabilities of small businesses and individuals.
- **Database/File Management** -These products are usually components of the database or operating system. They allow network administrators to set different levels of access and control to different users or user groups. Major flaws of these products and/or network administration features is their inability to protect the user from virus attacks.
- **Auditing Software** -Auditing software records and stores logs on server and data access. Auditing software is a powerful network management tool for detecting weak spots and security loopholes on the private network.
- **Virtual Private Networks (VPNs)** -VPNs are an amalgamation of intranet and extranet technologies to allow remote access by employees and lock out public network intruders (i.e., hackers). VPN security is crucial, as sensitive data is transmitted to remote corporate users.

Access Control Product Group

Access control tools enable network managers to restrict access and filter the data traveling across the network. Chief data access technologies include:

Firewalls

Firewalls are the most popular security product, with applications ranging from home desktop protection to worldwide corporate network protection. A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device or a software program running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet.

A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, data is routed between the networks; otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers-address filtering, by specific types of network traffic-protocol filtering, or by packet attribute or state.

Some users object to the fact that hardware firewall appliances eliminate access to the operating system. Significant disadvantage of software firewalls is that even high-end sophisticated multi-layer firewalls can be penetrated.

Proxy servers

When a user on the internal network attempts to connect to a server on the Internet, the proxy server sets up the connection and is the only system publicly advertised. Proxy servers should be used in conjunction with some form of packet filtering, or else clients and attackers alike might be able to go around the server.

Security Monitoring and Intrusion Detection Tools

These are software products that reside on gateway servers and constantly monitor for unauthorized access attempts. If a security intruder is detected, the application sends an intrusion alert message to potentially vulnerable users. These tools are effective in protecting a corporate network from external intruders and/or limiting the damage from the attack by immediately warning users.

Gap Technology Devices

Gap technology allows for a "disconnection" between two networks while allowing them to share resources or information. The difference between a firewall and a gap technology device is the following: a firewall is the logical disconnection of two physically connected networks, while a gap is a physical disconnection of two logically connected networks. Currently, there are three main categories of gap technology:

- **Real-Time Switch** -in a real-time switch architecture, two networks that are physically disconnected can share data as if they were connected. This seeming contradiction is achieved by adding a gap device that shuttles information back and forth between the two networks. In this case, the gap device is a hardware switch that can be physically connected to only one of the networks at a time. On a very basic level, the switch connects to one network, reads the waiting data, switches to the other network, and pushes the information

onto it. This switching happens at very high speeds, allowing for functional operation in a real-time environment.

- **One-Way Link** -a one-way link is the most straightforward gap configuration. It creates what is essentially a "read-only" network connection, which doesn't allow data to cross back into the source network. Like a real-time switch, it must be implemented in a hardware solution that physically prevents data from going the wrong way.
- **Network Switcher-** a network switcher is similar to a real-time switch, with the notable difference that it does not work in real time. A network switcher is typically implemented as a card with dual interfaces. Each interface is connected to a separate network, with only one interface active at a time. A proper implementation will segment all system resources, assigning some to each interface, with none belonging to both. In this way, storage that is assigned to one network is never accessible to the other network. This means that files and information retrieved from one network cannot inadvertently be put out on the other. If these files contain sensitive information, viruses, or malicious code, they cannot traverse this boundary.

Encryption Product Group

Encryption and decryption technologies, such as public/private key (PKP) and digital signatures, are used to guard data transmitted over the network. Within this product group, VPN, encryption enablers, and e-mail encryption are the key areas of product development.

PKI and Digital Signatures

PKI encryption works in relation to digital signatures. When the sender encrypts a message with his/her private key, any receiver with a sender public key can read it. When a digital signature is attached by a sender to a message encrypted in the receiver's public key, the receiver is the only one that can read the message and, at the same time, he/she is assured that the message was indeed sent by the sender.

PKI cryptography and digital signatures are applicable and widely available encryption/decryption technologies. They are mostly used when information is sent by e-mail and protect data as it travels through public networks (i.e. the Internet).