Anti-Virus

Small & Medium Businesses Network Security Guidelines

From
MicroWorld Technologies

Contents

The Threat Scenario

The Small and Medium Businesses contribute to around 68% of the world economy while making up for 80% of the employment. The security needs, issues and priorities of SMBs are different in many ways from that of large Business Houses.

While big enterprises have a well defined security mechanism in place with dedicated personnel to look after it, the scenario is a little different in SMBs since in comparison they are less organized, short-staffed and under equipped. They have a small number of IT staff who can manage to devote only a portion of their limited time towards network security.

Another major area of concern is the lack of user awareness owing to a significant presence of inexperienced, part-time employees. A recent study by MicroWorld Technologies showed that security awareness is 45% lesser among staff of smaller businesses in comparison with large enterprises.

One knows small businesses work on stringent standards of Service and Product Delivery models adhering to tight deadlines, as client demands are always on the higher side. Business Continuity is a vital factor for Mid-size organizations in retaining the clientele and fostering relationships. Security breaches and Virus infections in the internal network of organizations can be quite detrimental for their Business Continuity as they can bring down the entire function of the network to a grinding halt in a matter of few hours.

Current Threat Scenario:

- Rise in Organized crime
- Increasing Web Threats
- The use of legitimate websites to infect unsuspecting users
- Cybercrime takes a bite on Apple – targeting Mac users is beginning to prove that malware is not a Windows problem anymore
- Increasing threat to Mobile users
- Rise in Identity theft
- Pessimism reigns – public shows non-confidence in IT security with headline making incidents
- Stricter policing of the web – the takedown of major bot controlled machines sees security agencies waking up to the reality of cybercrime

Malware and more...

Virus

A typical computer Virus is a malicious program that destroys and alters files and folders, while replicating on its own. It usually attaches or inserts itself into an executable file or the boot sector of a disk.

Network Worms

This Malware spreads via P2P File Sharing, LAN, WAN and over the Internet using file sharing programs like Kazaa. A worm wriggling into a vulnerable computer of a large network will send requests to all other machines in order to propagate it.

Trojan

A Trojan refers to a program or a file that may look harmless otherwise, but carries a malicious component in it. Regular Trojans do not replicate themselves, but can be highly destructive, harm applications and threaten your Data Integrity. A MicroWorld study in September 2006 found that 31% of malware caught in SMBs belong to different Trojan families.

Trojan Downloaders

This breed downloads other Viruses, Worms and Trojans into the victim's machine from the Internet. Often they turn off the AntiVirus and Firewall in the system before bringing in new malware!

Trojan Clickers

Trojan Clickers redirect victim's machines to specific websites or other resources on the Internet. They make this possible by tampering with Windows HOSTS file to reroute regular web requests towards websites they wish. Trojan Clickers are widely used in increasing the hit-count of specific websites or for launching Denial of Service (DOS) attacks.

What are today's Business Demands

- Email, Text Chat, Web Browsing, File Sharing, Games
- Voice, Audio, Video, Tele-presence, Telemedicine
- Web Services (Web 2.0 aka Social Networking, Blogs)

Users To Enjoy Mobility

- Any service from any device on any network
- Seamless mobility across devices and networks
- Strong but easy user authentication.

Reliability and Security of Networks.

Pharming Trojans

This breed is similar to Trojan Clickers and is used in a dangerous attack called 'Pharming'. When an employee from your company's Finance Department accesses the website of the official bank to do a business transaction, he could unwittingly open a spoof website created by scamsters, where he gives away confidential financial information. They do this by making changes in the DNS settings.

Keyloggers

Keyloggers remain silent in a compromised computer and capture usernames and passwords when a user logs on to the websites of Financial Institutions, Banks and Credit Card Companies. The Information thus stolen is mailed to the author of the Malware. Some of the more evolved ones can take screenshots and capture mouse clicks too. This malicious code is a core component in Password Stealing Trojans.
Keyloggers can pose a dangerous threat to the Data Integrity of SMBs. If they manage to steal the email ID and password of a senior executive, all of his or her mail communication can be spied on, day in and day out.

Backdoor

This Malware is hooked into the victim's system by an intruder, in order to gain Access and Control of it. IRC (Internet Relay Chat) channels are widely used by Backdoors to connect to the attacker and take orders from the criminal who could be sitting just about anywhere in the world! Using Backdoors, the attacker can work on the compromised computer like his own desktop and execute commands – all this without the users knowledge.

Botnets

The term bot is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the Internet, without you knowing it.
Criminals typically use bots to infect large numbers of computers. These computers form a network, or a botnet.
Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If your computer becomes part of a botnet, your computer might slow down and you might inadvertently be helping criminals.

Rootkit

A Rootkit is used by malicious programs to hide running processes, files or system data, so that Security Applications do not detect their presence in the computer. They modify parts of the Operating System, install themselves as drivers or kernel modules in order to achieve deep penetration in the computer. It's the favored hiding mechanism for many recent Backdoors and Trojans.

Spyware

Spyware is a risky, malicious program typically bundled as a hidden part of freeware or shareware programs, downloaded from the Internet. It spies on user activities on computers and sends that information over the Internet to the Malware author. Spyware eats up system memory, damages its functioning, sneaks into sensitive, Personal Financial Information like Credit Card numbers and passwords.

Adware

Adware are nasty software programs that pester your computer screens with countless pop-up advertisements. Often they push you to the limits in their attempts to make you visit certain websites, buy tacky products online or join scam services. They can cause system crashing and rob your computing resources and bandwidth, all the while being a perpetual nuisance as well.

Parameters affecting the business demands

For business continuity and fast response, your employees, customers & partners (may) need access to the following:

- Increased Access to Sensitive Information
- Mission-critical network
- Mobile and remote devices
- Wide variety of storage devices
- Interoperability

2011 has been a phenomenal year for hackers and what we have witnessed is a sharp curve in attacks that's predominantly aimed towards large enterprises. With hackers taking advantage of various vulnerabilities within Windows OS's and third party applications, it goes to show the extent to which malware can be created. While the impact of the Stuxnet malware is old news – there have been bigger instances where enterprises have lost by the numbers. Take for example the breach of Sony Corporation – over 1 million user passwords were stolen via SQL Injection. To top it off, the passwords were stored in plaintext without any sort of encryption. Other instances include – hack on HBGary, Google, Sony and a handful more noteworthy companies. It goes without saying – in today's day and age, data theft and industrial espionage is of all importance.

Another great insight can be acquired by studying the recent phishing exercise carried out by KnowBe4 among Small and Medium Enterprises. The tests were basically carried out on 3,400 companies where emails were delivered to 29,000 recipients at 3,037 business units; individuals who clicked the link were directed to a landing page which then informed them about the simulated phishing attack.

"Any business that provides access to email or access to its networks via the Internet is only as safe from cybercrime to the degree that its employees are trained to avoid phishing emails and other cyber heist schemes. The more employees within an organization that use email or go online, the greater the risk of exposure to cybercrime" - Stu Sjouwerman (KnowBe4 Founder and CEO).

According to the research carried out, the most Phish-prone industries are:

Travel	– 25%
Education	– 22.92%
Financial Services	– 22.69%
Government Services	– 21.23%
IT Services	– 20.44%

Spam and Social Networking Threats

Wading through the clutter of Spam is one of the biggest challenges faced by employees of SMBs on a daily basis. Accidentally deleting important and legitimate mails in that process is another issue. Bandwidth issues, Storage Concerns, Loss of Productive hours and Distribution of Malware are a slew of other concerns for organizations, stemming out of Spam mails. Mail addresses posted on the web and Chat Services are quickly harvested by spammers using an array of techniques to send large numbers of unsolicited emails to those addresses.

Botnets have always been used to send high volumes of spam. Technically speaking, the distribution of malware was aimed to increase the number of spam mails. However this is not the case now as the last couple of months clearly depict a decreasing trend in the number of spam being sent out. However, there are a handful of other ways for botnets to operate. These would clearly include – large scale banking fraud, account theft of email and social networking sites, Distributed Denial of Service (DDOS) – to name a few.

Various instances that are used for tricking users into opening attachments would include:

- Courier (UPS, Fedex, DHL) package notifications – package notification that is due or help up, with details attached within the mail
- Hotel charge error – incorrect hotel bill that would need to be corrected by opening the attached document
- The "map of love" – promising juicy information about global sites of "interest" in the attached map
- Credit card errors – an incorrect credit transaction needs to be reversed with more details in the attached
- HP scanner doc – a document scanned on the office scanner has been delivered
- Inter-company invoice – includes a confusing message about an attached invoice
- NACHA errors – an inter-banking transaction has been rejected. The reasons for the rejection are in the attached document

Pharmacy spammers tend to use direct emails which explicitly state the types of medicines being offered. Even with most spams that end up within the junk email folders, there are a selective few who would still be interested in opening such mails. With that said, Facebook continues to draw attention of malware writers. The month of October saw a series of campaigns or scams that were spread as events with catchy titles-

- First 40,000 participants get an iPhone free
- First 30,000 that signup get a free pair of Beats by Dre headphones
- First 2,000 participants to like this page will get a Facebook Phone free
- First 20,000 participants will get a free Facebook shoe

Over 100 billion US Dollars is what global business houses loose by way of dent in productivity and wastage of technology which comes in as a direct and immediate impact of spam, while its second and third levels of ramifications on the economy could be much deeper and wider.

Network Hacking

Port Scanning is the most popular searching technique used by attackers to identify vulnerable systems and services in a network. Many services work with TCP and UDP ports and there are as many as 6000 ports currently used in networking.

In Port Scan, an attacker sends messages to targeted ports and based on the response it generates, probes deeper for vulnerabilities. TCP ports are targeted the most as they are connection oriented and normally give immediate response to the Intruder.

Some methodologies used in Port Scan are given below

SOCKS Port Probe

SOCKS is used in a network to facilitate sharing of Internet connection among multiple systems. There's a good possibility for erroneous configuration of some of these ports by some users, creating arbitrary sources and destinations. This helps a cyber criminal to hide his location and access the Internet through the victim's machine.

Stealth Scan

Normal Port Scanning is done with the help of a series of packets rapidly fired at the host. But 'very slow scanning' can be used as a stealth technique to avoid detection. Another such method is called Inverse Mapping, where the attacker finds all hosts in the system by employing "host unreachable" ICMP-messages.

Fragmented Packet Port Scan

This is done by breaking a TCP header into several IP fragments. Many firewalls can be tricked by this technique as they normally try to match the whole TCP header to identify an attempt of intrusion.

Insider Threats

Ever since information has turned digital, data has never been easier to get hold of. Think about it - there used to be a time when hackers used to hack just for recognition. Come to think of it, cybercrime wasn't even a word that was used to link hackers. But if you compare it with the current trending scenario, we will notice a drastic change within the hacking community. Over the years targeted attacks have grown significantly where corporate organizations have had to beef up their current security solutions to thwart web based attacks. Having said that, there are still instances where organizations get pawned or owned by hackers. Question is – would you hold employees responsible for the spreading of infection? With the widespread increase of fraudulent, malicious and scamming sites, it is inevitable for every employee within the organization to understand this growing threat. The question that needs to be answered here is – can you trust an employee to not visit a website that has been compromised and infected by malware? To be precise, 99% of the infections that occur within organizations happen due to inadequate security solutions in place. It's just not email security that needs to be taken care of but securing an employee's browsing habits is just as important.

Among Small and Medium Businesses it is said, close to 40% suffered from a security breach due to bad surfing habits. This basically resulted in navigating to websites that were home to malware, malicious downloads that might have been corrupted by malicious code. The aspect that needs to be understood is that the Internet is more like a hive for malware and cybercriminals are always on the hunt to fish out unsuspecting users. What remains a worrying concern is the fact that a handful of organizations are not implementing the needed precautions that would prevent employees from clicking a malicious link or even browse unwanted sites.

According to research held by CSIS (Center for Strategic and International Studies), it is seen even in the event of infections, a number of users who use web monitoring software do not consider the importance of considering their network as the main vector for deploying the necessary solution or policies. Over 52% of SMBs state that it isn't in their top priority list to set up a perimeter against web threats. Statistically speaking, a total of 24% of IT Administrators who did consider setting up a perimeter deployed it mainly to enforce employee productivity while 15% used policies to maintain the overall speed of the network and just 13% used policies to forbid employees from accessing illegitimate sites. However, the question that still needs to be answered is – are these reasons valid enough for organizations to use just a web monitoring software? Doesn't security play a major role?

The results however, clearly show the overall lack of awareness of what web monitoring software is capable of. Securing the network or endpoints from malicious downloads, websites or even endpoints

such as USB ports should be of top priority. Probably superseding concerns such as bandwidth management and employee productivity. The survey also found a high number of organizations that didn't consider using filtering or even a web monitoring software. With the increasing number of threats this becomes a major concern as company as well as user information can easily be siphoned off without knowledge.

What needs to be looked into here is – a proper deployment of web monitoring software that co-exists with a robust security suite which provides an additional layer of defense against web threats. The need to secure an employee from accessing malicious or illegitimate sites will definitely go a long way for SMBs in maintaining a proper balance that would more or less nullify the overall risks an employee creates when accessing the World Wide Web.

E-mail poses other risks as well. Consider the documents and e-mails your company sends—would you want that information made public? More than half of those surveyed access their work e-mail accounts via a public wireless hotspot; 52 percent access their work e-mail via a public computer.

Mobile devices are also a concern and about 65 percent of respondents frequently or sometimes leave their workplace carrying a mobile device such as a laptop, smart phone or USB flash drives that hold sensitive information related to their jobs: customer data, Social Security or credit card numbers, company financials and competitively sensitive information like product plans. Of those surveyed, 8 percent have lost a mobile device that contained corporate or organizational information.

At two-thirds of respondents' companies, wireless connections are available in conference rooms and guest offices; of those, 19 percent reported that access to the corporate network is completely open and no credentials are required.

What are Endpoints?

- Endpoints, in simple terminology, comprises of basically devices that either have communicational capability and/or storage capability.
- Endpoints could be Hardware or software in nature

Integrated approach to security

The ideal solution plan for Mid-size firms looking to protect their Information Systems from a variety threats mentioned so far would be to rely on comprehensive AntiVirus, AntiSpam and Content Security Solutions with a Central Management Console. A powerful Network Firewall is also a necessity to defend against intrusions. The system or systems should scan all HTTP and FTP traffic for malicious code, block spam and phishing and provide policy based Access Control for the entire organization.

Let's first see what all capabilities an AntiVirus, AntiSpam and Content Security solution should have.

Real-Time Malware Scanning with the Earliest Detection of new threats

First things first - The prime job of an AntiVirus is to detect and block all sorts of malware. It should check e-mails and websites in real-time for Viruses, Worms, Trojans, Spyware, Adware, Keyloggers, Backdoors, Rootkits and more. It must have the fastest and earliest updating database for detection and removal of all kinds of Malware including latest exploits targeting vulnerabilities in Operating Systems and other Software Applications.

Behavioral and Intentional Analysis

The system should employ a highly sophisticated Behavior and Intention Analysis method to identify unknown Viruses and Worms. This means the AntiVirus will proactively block even that malicious code, whose signature is not present in the AntiVirus Database.

Integrated Security Policy Enforcement

The Management Console of the software must enable the network administrator to view and access the entire network architecture, including activities at different workstations. Features should allow the administrator to distribute new updates across the network. Options are required to block ActiveX controls and stop exploit codes and Trojan Droppers targeting browser vulnerabilities. The software should make sure that no unwanted program is installed in your computer in deceptive ways.

Remote Web Administration

The Management Console should have a web interface, so the Network Administrator can access the Console from a remote location. This will enable the Administrator to manage the security of a company even while being away from the office.

Rootkit Tracing and Removal
An ideal AntiVirus comes with the power to detect and remove Rootkit components in the system so that Worms and Trojans cannot hide their presence.

Protection against Spyware and Adware
The software must provide continuously updated protection against Spyware and Adware that mushroom in many forms and names every passing day. The software should be capable of repairing damages done to the system by these Riskwares.

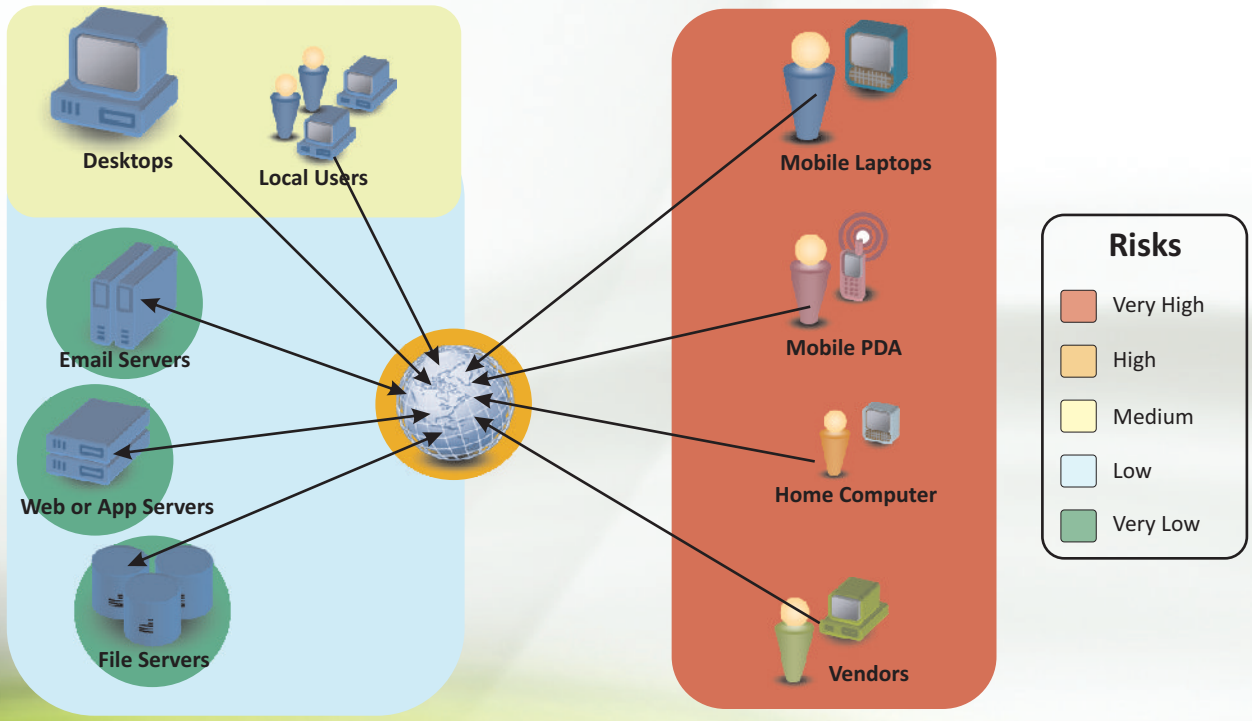
Integrated Web Access Policy Enforcement and Management

- **Policy Implementation and Control**
  Options should be provided for the formulation and implementation of advanced policies containing many categories for Content Security and Web Access control.

- **Whitelisting**
  Once you add a user or IP to the whitelist, content checks will not be done on those entities.

- **Blocking all inappropriate and non-productive websites**
  A combination of technologies should be available for blocking all non-productive, harmful and unsuitable websites at a single point. The process of website filtering works on the basis of occurrence of certain 'robable'words like sex, gambling, chat room and more within web pages. If the word count goes beyond a certain threshold level, then the website in question needs to be blocked and added to blacklist.

Typical Computational/Communicational Endpoints



Protection against Intrusion and Hacking

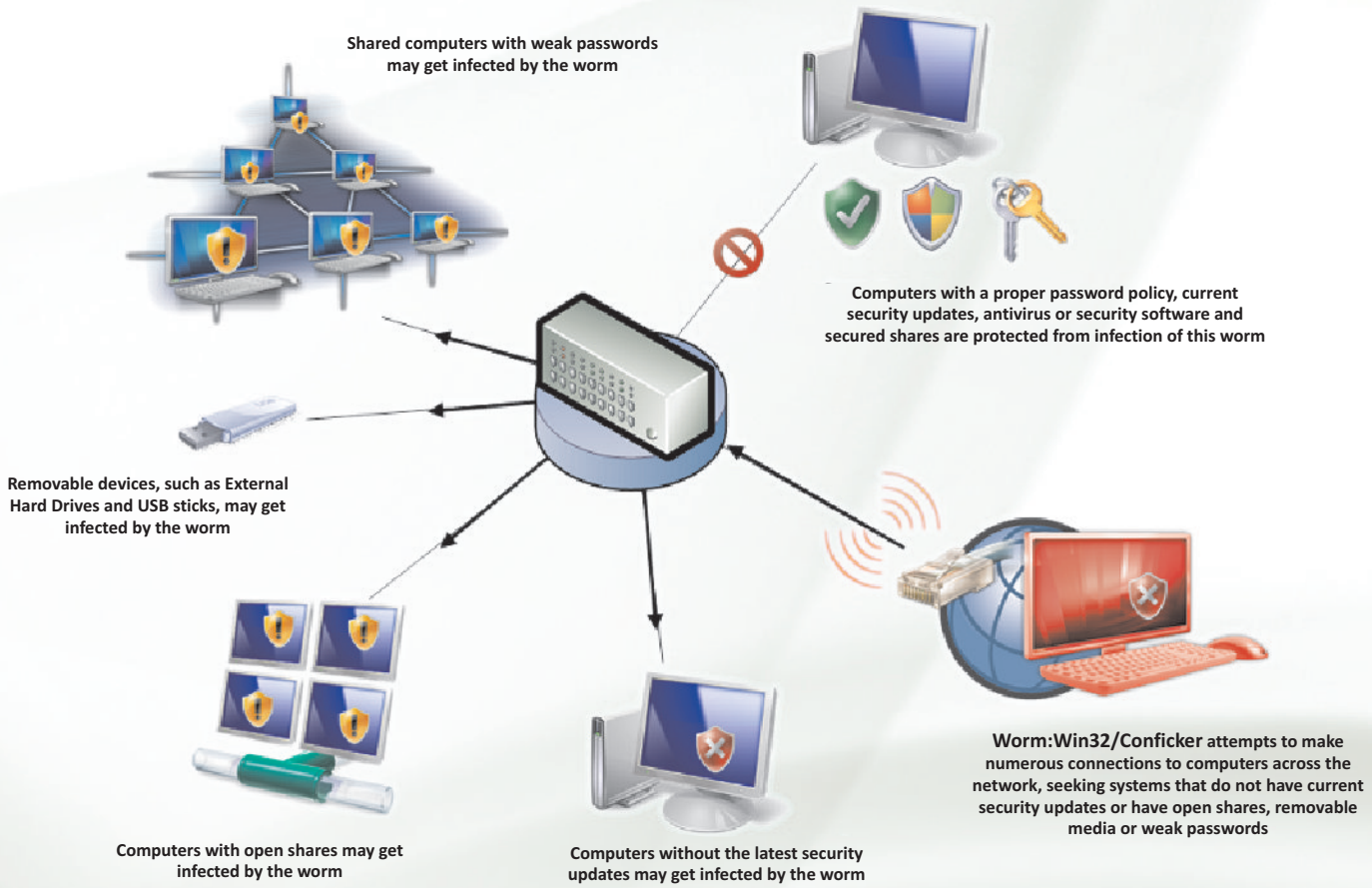
The ideal firewall for an SMB network should offer customizable security with user-defined rules for Packet Filtering and Access Control. It must allow the administrator to create Rules based on non-IP protocols such as ARP, whilst supporting multiple network adapter configurations.
Some of the must haves of an ideal firewall for SMBs are given below.

Port Monitoring

It should prevent Port Scanning by network attackers and alerts you of any such attempts. Ideally, the software needs to allow the user to specify Source and Destination ports, and Source and Destination IP addresses. This enables you to enforce Communication Control on specified ports and systems.

Network Data Filtering

An ideal firewall monitors and filters IP and Non-IP Network Traffic so that no intrusion takes place in the company's internal networks.



Active Network Monitoring
You should be able to view details of all TCP connections on your system. Information like Process, Protocol, Local Address, Remote Address, Status and Start Time needs to be displayed in detail.

Filtering Level
It should provide options for Application and Packet Level filtering. Application Level helps you set up Rules for a particular Application. Packet Level provides filtering of incoming and outgoing data packets.

User-defined Rules
The Firewall has to provide a powerful Traffic Filtering system with user-defined processing Rules. Option must allow the users to define Rules according to his or her requirements and implement customized traffic filtering.

Preset Rules
The solution must provide a set of pre-defined Rules so that a newly installed system gets a head-start in enforcing Data Traffic Control. The different types of rules are ARP, DHCP & BOOTP, DNS, E-mail, WWW, News, Net Bios, FTP, ICMP, ICQ, Telnet & SSH, IRC, MSN, and VPN.

Stealth Mode
This option gives you the power to surf the Internet invisibly, without letting other online users see you. When online, your computer constantly receives and responds to information requests from other computers. In stealth mode your computer will not respond to this flow of queries and requests, and thereby reduces the possibility of system hacking significantly.

Comprehensive Logs
The Firewall needs to store log information detailing programs involved in outgoing/incoming traffic, Communication Protocols used, Source and Destination IP addresses, Direction of Traffic and action taken depending on Rules in force. In addition, it needs to maintain an Event Log that details user events – e.g. changing security levels, loading Rules, firewall shutdown etc.

Real-time Reports
The firewall should provide clear, concise graphical and non-graphical reports on internal and external Data Traffic. Diverse reports based on Application, Expert Rule, Zone Rule, IP and Date are available along with graphs having different styles like Bar, Pie, Line and alike. These reports enable the Network Administrator to quickly analyze the patterns of data movement and to devise strategies based on them.

Anti-Virus / Anti-Spyware

- Real-Time AV Scanning
- Spyware, Adware, Keylogger, & Rootkit Blocker
- Suspicious Application Detection
- Registry Monitoring
- Protection against web based threats
- Protection against email based threats
- Spyware and rootkit detection and removal
- Ability to safely remove infections & restore system files effectively
- Detect, prevent and remove malicious code & Vulnerability-based protection

The software must offer default categories like Pornography, Gambling and Ratings Based Blocking. As an administrator, you should have the ability to create as many new categories as required to control the types of websites that you deem unsuitable for the firm.

Pop-Up Ad Blocker
The system must stop pop-up advertisements that plague your computer screen. You must have an option for whitelisting Pop-Ups from specific websites and also have a 'hot key' option to temporarily allow pop-ups.

Protect Privacy and Confidentiality
The application should protect your privacy and prevent access to confidential information. It should be capable of erasing links of visited websites and entries made in online forms. It should allow the user to schedule browser clean-up for Cookies, Plugins, History, Cache, and links to most recent files and images opened

Multi-tier Mail Protection

The security software at the Mail Server should have a Multi-layered Spam Control mechanism. It should include technologies like,

- **Real-Time Black List (RBL)**
  RBL is a DNS Server that lists IP Addresses of known Spam sending machines. If the contacting IP is found to be in one of the blacklisted categories, the connection is terminated.
- **MX/A DNS Record Verification**
  The domain part of the email address is checked to see if it has a DNS MX (Mail Server) and/or IP record, as it is typical of spammers to use non-existent domains in their emails.
- **Reverse DNS**
  A reverse DNS check is performed to see if the connecting IP resolves to a valid domain name before accepting or rejecting the email.
- **Grey Listing**
  A new email from an unknown sender is kept out for a certain amount of time before accepting it. The logic is that if it is a legitimate mail, the Mail Server will try to resend it, while in most cases spammers won't.
- **Sender Policy Framework (SPF)**
  Sender Policy Framework is a world standard that helps to prevent forgery of sender address, and hence works as a powerful mechanism to stop Phishing mails.
- **Self Learning, Adaptive technology in Spam Control**
  The need is for a Spam Control system that works on the principles of Artificial Intelligence. It should analyze each mail according to the Behavioral Patterns of the user and take an informed decision based on that. Such a system will show the best accuracy in weeding out Spam.

Conclusion

Threats faced by SMBs are many and multi-dimensional. As aspiring firms are trying to make it big in the cut-throat competition out there, it is imperative that mid-sized businesses recognize the importance of safeguarding their Information Systems. A comprehensive solution plan that offers the best-of-breed protection in every aspect of security is the need of the hour. It should provide centralized management, enable Integrated Policy Enforcement and reduce the administrative over-head to a near zero. Once you achieve that, you can safely say that you have a secure IT infrastructure for your business.

About eScan

eScan, the world's first Real-time Anti-Virus and Content Security software for desktops and servers is developed and marketed by MicroWorld. It is powered by innovative and futuristic technologies, such as MWL Technology, DIRC Technology, NILP Technology, and sophisticated Anti-Virus Heuristic Algorithms that not only provide protection from current threats, but can also provide proactive protection against evolving threats. It has achieved several certifications and awards from some of the most prestigious testing bodies, notable among them being Virus Bulletin, AV-Comparatives, West Coast Labs (Checkmark), ICSA, and PCSL labs. Combining the power of various technologies, eScan provides Multilevel Real-time Protection to Computers and Networks. For more information visit: www.escanav.com.