

A SECURITY MANAGEMENT SYSTEM DESIGN

A THESIS SUBMITTED TO  
THE GRADUATE SCHOOL OF SOCIAL SCIENCES  
OF  
MIDDLE EAST TECHNICAL UNIVERSITY

BY

HULUSİ ÖNDER

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR  
THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION

JULY 2007

Approval of the Graduate School of Social Sciences

---

Prof.Dr.Sencer AYATA  
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Business Administration.

---

Prof.Dr. Can Şınga MUGAN  
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Business Administration.

---

Assoc.Prof.Dr. Zeynep ONAY  
Supervisor

**Examining Committee Members**

Prof.Dr. Semih BİLGİN (METU,EEE) \_\_\_\_\_

Assoc.Prof.Dr. Onur DEMİRÖRS (METU,II) \_\_\_\_\_

Assoc.Prof.Dr. Zeynep ONAY (METU,BA) \_\_\_\_\_

**I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.**

Name, Last name : Hulusi ÖNDER

Signature :

# **ABSTRACT**

## **A SECURITY MANAGEMENT SYSTEM DESIGN**

**ÖNDER, HULUSİ**

MBA, Department of Business Administration

Supervisor: Assoc.Prof.Dr. Zeynep ONAY

July 2007, 99 pages

This thesis analyzes the difficulties of managing the security of an enterprise network. The problem that this thesis study deals with is the central management of a large number and variety of services that provide organization-wide network and information security. This study addresses two problem areas: how to better manage the security of a network, and how to explain the security issues to upper management better.

The study proposes a Security Management System (SMS) to be used for network security management, monitoring and reporting purposes. The system is a custom made, central management solution, which combines the critical performance indicators of the security devices and presents the results via web pages.

**Keywords:** Centralized Security Management, Monitoring Network Security, Log Handling.

# ÖZ

## GÜVENLİK YÖNETİM SİSTEMİ TASARIMI

ÖNDER, HULUSİ

İşletme Yüksek Lisansı , Sosyal Bilimler Enstitüsü

Tez Yöneticisi: Doç. Dr. Zeynep ONAY

Temmuz 2007, 99 sayfa

Bu çalışma, ağ güvenlik yönetiminde karşılaşılan sorunları analiz etmiştir. Bu çalışmada ele alınan sorun, kurumsal ağ ve bilgi güvenliği sağlamak maksadıyla kullanılan çok sayıda ve çeşitlilikteki güvenlik yazılım ve donanımların merkezi olarak yönetimidir. Güvenlik yönetiminin nasıl daha kolaylaştırılabileceği ve güvenlik ile ilgili konuların üst yönetim kademesine nasıl daha anlaşılır şekilde anlatılabileceği hususları araştırılmıştır.

Bu çalışma neticesinde ağ güvenlik yönetimi, kayıt izleme ve raporlama işlemlerinde kullanılmak üzere geliştirilen Güvenlik Yönetim Sisteminin (GYS) kullanımı önerilmektedir. Bu sistem, güvenlik cihazlarının kritik performans göstergelerini biraraya getirerek, web sayfaları aracılığı ile kullanıcıların kullanımına sunmaktadır.

Anahtar Kelimeler: Merkezi Güvenlik Yönetimi, Ağ Güvenliği İzleme, Kayıt İzleme.

## ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my supervisor Assoc.Prof.Dr. Zeynep ONAY for her excellent guidance, advice, criticism, encouragements and insight throughout the research. I also would like to thank Prof.Dr. Semih BİLGİN and Assoc.Prof.Dr. Onur DEMİRÖRS for kindly accepting to take part on my jury and for their critical contributions, which enriched my thesis.

I also want to acknowledge the invaluable support of my department head in Turkish General Staff Headquarters, Lt.Cd. Cem Ali DÜNDAR. Without his support and encouragement, I would not have a chance to be part of the MBA program in METU. The help and support of my coworkers in my department; Bilgen ÖZHAN, Dursun GÖKDEMİR and Erhan SAKALLI is unforgettable. I would like to thank them for helping me throughout the MBA education and my thesis study.

I would like to express my love and appreciation to my mother Ayşe ÖNDER and my fiancée Demet ÇALIŞKAN, and my entire family for being with me during my MBA education and my thesis study.

## TABLE OF CONTENTS

ABSTRACT .....	iii
ÖZ.....	iv
ACKNOWLEDGMENTS .....	v
TABLE OF CONTENTS.....	vi
LIST OF FIGURES .....	x
LIST OF TABLES .....	xi
1. INTRODUCTION .....	1
1.1. System Security .....	1
1.2. Statement of the Problem.....	2
1.3. Aim of the Study .....	6
1.4. Scope of the Study .....	7
2. LITERATURE REVIEW.....	8
2.1. The Need for Security .....	8
2.2. Enterprise Security Management .....	10
2.2.1. Common Practices .....	10
2.2.2. Enlargement Difficulties.....	11
2.2.3. Log Handling.....	11
2.2.4. Complexity Problem and Management Difficulties .....	12
2.3. Designing a Secure Network.....	14
2.3.1. Design Goals.....	14
2.3.2. The Concept of Defense-in-Depth.....	15
2.3.3. Public – Demilitarized Zone (DMZ) - Private Network Layout.....	16
2.4. Security Administrator Responsibilities .....	18
2.4.1. Definition.....	18
2.4.2. Tasks of Security Administrators .....	18
2.4.3. Challenges of Security Administrators .....	19

2.4.4.	Ways of Serving Better.....	20
2.5.	Monitoring .....	21
2.5.1.	The Importance of Monitoring .....	21
2.5.2.	The Need for Human Intervention.....	23
2.6.	Incident Handling.....	24
2.7.	Upper Management’s Involvement in Security .....	25
2.7.1.	Importance of Security Awareness.....	25
2.7.2.	Responsibilities of Upper Management.....	26
2.7.3.	Upper Management Commitment to Security .....	27
2.7.4.	The Evaluation of Security Investments.....	27
2.8.	Conclusion .....	28
3.	DETERMINATION OF REQUIREMENTS AND SECURITY MANAGEMENT	30
3.1.	Determination of Requirements.....	30
3.2.	Security Management .....	31
3.2.1.	Network Security Background .....	31
3.2.2.	Network Functioning and Server Status .....	34
3.2.2.1	Ping Command.....	36
3.2.2.2	Service Status.....	38
3.2.2.3	Disk Space .....	39
3.2.2.4	Bandwidth Usage .....	40
3.2.3.	Firewalls .....	40
3.2.4.	Intrusion Detection / Prevention Systems (IDS/IPS).....	44
3.2.5.	Anti-Virus Software.....	47
3.2.6.	Updates .....	49
3.3.	Reports .....	51
4.	DESIGN OF THE SECURITY MANAGEMENT SYSTEM.....	53
4.1.	Introduction.....	53
4.2.	Model Network .....	55
4.2.1.	Firewall.....	56
4.2.2.	Intrusion Detection System (IDS) .....	57



4.2.3.	Anti-Virus Software.....	58
4.2.4.	Update Monitoring.....	58
4.2.5.	Network Monitoring .....	59
4.2.6.	Service Status Monitoring .....	59
4.2.7.	Disk Space Monitoring .....	59
4.2.8.	Bandwidth Monitoring.....	60
4.3.	System Configuration .....	60
4.4.	Security Management System (SMS).....	61
4.4.1.	Design Goals of SMS .....	61
4.4.2.	Organization of the Main Page of SMS.....	63
4.4.3.	Internal Firewall.....	64
4.4.4.	External Firewall .....	67
4.4.5.	Intrusion Detection System (IDS) .....	70
4.4.6.	Anti-Virus System .....	72
4.4.7.	Network Monitoring .....	75
4.4.8.	Bandwidth Monitoring.....	76
4.4.9.	Disk Space Monitoring .....	78
4.4.10.	Service Status Monitoring .....	80
4.4.11.	Update Status Monitoring.....	82
4.4.12.	Reports.....	84
4.5.	Conclusion .....	85
5.	DISCUSSION AND CONCLUSION.....	86
5.1.	Discussion .....	86
5.1.1.	Better Convenience.....	87
5.1.2.	Reduced Time for Monitoring .....	88
5.1.3.	Centralized Presentation of the Logs .....	89
5.1.4.	User-friendly Interface and Ease of Navigation .....	89
5.1.5.	Better Way of Troubleshooting .....	90
5.1.6.	Modular and Scalable Design .....	90
5.1.7.	Centralized Storage of Reports.....	90

5.2. Conclusion .....	91
REFERENCES .....	95

## LIST OF FIGURES

Figure 2.1	Logical Flow of Security Information Management .....	20
Figure 3.1	Basic Network Diagram.....	35
Figure 3.2	Demonstration of the Use of Ping Tool. ....	37
Figure 3.3	Services Control Interface in Windows Operating Systems.....	39
Figure 3.4	WSUS installation in a network.....	50
Figure 4.1	Security Management System Model and the Sections of the SMS Main Page.....	53
Figure 4.2	Sample Network Layout. ....	56
Figure 4.3	Main Page of SMS .....	62
Figure 4.4	Web page of the Internal Firewall.....	65
Figure 4.5	Web page of the External Firewall .....	69
Figure 4.6	Web page of the IDS .....	71
Figure 4.7	Web page of the Anti-Virus Software.....	74
Figure 4.8	Web page of the Network Monitoring Software.....	76
Figure 4.9	Web page of the Bandwidth Monitoring Software .....	78
Figure 4.10	Web page of the Disk Space Monitoring Software .....	79
Figure 4.11	Web page of the Service Status Monitoring Software.....	81
Figure 4.12	Web page of the Update Status Monitoring Software .....	83
Figure 4.13	Web page of the Reports.....	84

## LIST OF TABLES

Table 2.1	Tasks of a Security Administrator.....	19
Table 2.2	Advices to Administrators.....	21
Table 5.1	Comparison of SMS with TriGeo's SIM.....	93

# **CHAPTER 1**

## **INTRODUCTION**

### **1.1. System Security**

The digital age has emerged with a variety of benefits to organizations and individuals. Information technologies are becoming more widely used everyday. Networking of computers and the invention of the Internet were cornerstones of the new technology age; however transferring confidential data and transactions from paper and pen based environments to computer systems does not always happen as expected. As networks and computer systems become pervasive, vulnerabilities, flaws, security threats and risks grow more rapidly than in many other technologies. The types of threats are various. Security specialists and experts are trying to create solutions for each type of threat through different methods like attack signatures and heuristic approaches for prevention. However, as solutions are created, new types of threats emerge, such as spam mails, spywares, adwares, worms and trojans.

Prevention is more difficult than being on the opposite side in the area of computer security. Finding out a vulnerability and exploiting it is more alluring than trying to maintain a network's security by examining the logs, updating the systems or applying patches.

The Internet is such a phenomenon that an organization today cannot survive without it, but on the other hand, living with the Internet makes organization prone to threats that did not exist before. Even though governments are enacting laws and regulations to minimize the so called 'digital crimes', the nature of digital crimes and the digital environment makes it nearly impossible to catch the attackers. Organizations are accessible from computers all over the world through the Internet.

Although legal precautions against cybercrime have been taken like the Convention on Cyber Crime (Council of Europe, 2001; Ankara Emniyet Müdürlüğü, 2001), it is difficult to enforce them in a digital environment. Based on these facts, organizations should apply the best security precautions they can attain, and invest in information security. This situation leaves them the option: To live with the Internet and networking but secure it as much as possible. Bruce McConnell emphasizes defense against cybercrime:

“Organizations must rely on their own defenses for now. Governments, industry and civil society must work together to develop consistent and enforceable national laws to deter future crime in cyberspace.” (as cited in Armstrong, 2001, p.33-34)

## **1.2. Statement of the Problem**

The problem of security management has many facets. The most important one is complexity. As more complex and quality software is produced and used, vulnerabilities increase. Furthermore, there are many malicious computer experts, called hackers or crackers, ready to find out these vulnerabilities and exploit them. Hackers have several motives, some of them are looking for fame and money, others are doing it just out of curiosity. However, the consequences of the attacks, independent of the attackers' motive, are always costly for organizations. The complexity issue is a problem that is not likely to go away soon, but there are other problem areas that can be mitigated with careful configuration and management: Analysis of security logs, central management of security devices, and presentation of the performance parameters of computer security devices to upper management.

Several application and security servers are in the jurisdiction of the security administrator. Besides their dedicated tasks, these servers spend a great amount of their Central Processing Unit (CPU) power for producing logs about activities in their given tasks. These logs may reach enormous amounts in many servers if they are not

handled properly. Besides, all these logs are useless if not taken into consideration and analyzed by administrators. The default installation of security equipment generally provides a configuration interface and log investigation interface to the administrator. However, most of these interfaces are only available on the server where they are installed. Logging on to several servers and using different interfaces everyday is a painful and tiresome task for any administrator.

Security measures in computer systems work against the usability of the systems. As security hardening is applied, users lose one or more functionality, or it becomes more difficult to complete a task, or to reach a file on the web. For example; in a network domain, if users are not forced to change their passwords periodically, most of them will not change their passwords regularly, or have security concerns about keeping the same password for a long time. They would rather not spend time in changing the passwords and remembering the new passwords when they log on to the domain. The laws of security recommend the opposite, and dictate that passwords must be changed regularly. As administrators decide to enforce the security policy of the organization to comply with security recommendations, users will be forced to choose complex passwords instead of easy ones, and they will be in a situation to change them periodically. This change in policy can be a big leap for the organization in securing the network. Although the network becomes more secure, the users may not like it since it brings an additional burden to their workload.

Security usually contradicts the user-friendliness of systems. Users would prefer the easy but non-secure way of completing a task to the difficult but secure one. The nature of security makes security administration more difficult, since users are not security oriented by default, not deliberately but instinctively.

Besides the environmental difficulties and user-related issues, there is another important problem in the implementation of security: expert and adept security

administrators are hard to find. Most organizations suffer from the inadequacy and reluctance of their security personnel as much as they suffer from other organizational problems. Security is not a task that can be finished in a given amount of time, rather it is an ongoing and never-ending process, in which human interaction is needed, and cannot yet be replaced with computer technology. One of the main objectives of technological improvements in computer security is to replace the human factor with computers in order to ease the task. However, a total solution to replace human decision-making capabilities in security management with a computerized one is not yet available. Thus, computer security management still needs experienced, skillful and well-educated administrators.

Top-level management involvement is another critical problem area. Upper management should be aware of the importance of security and support security administrators in their quest to establish a solid and secure network. However, in many organizations, the situation is not as it should be; Top-level management is not well informed about the importance of the security; therefore, they have prejudices and biases about security and the security personnel. These biases lead to ill-advised decisions that may jeopardize the security of the organization. For example, there is a common management prejudice: “We have firewalls, intrusion detection systems and anti-virus software, we should be safe and secure, nothing may impend our assets”. Security administrators should try to get top management involvement in security issues through the help of meaningful reports, justifying investments in system security.

Managers who are in charge of supplying the resources for security investments do not easily realize the importance or the effectiveness of security devices. When some amount of money is invested in an information system application, such as a new printing server or a new e-mail server, every member of that organization can easily realize the benefits of this investment, but the situation is



not the same for a security investment. Nobody, other than the security administrators and security managers in the organization realize the need for that investment, and very few realize what difference it makes, or what kind of benefits it brings to the organization.

Defense against threats to the network requires the use of security solutions and products. When new security equipment is installed in an organization's network, the workload of the security administrators increases. The new security solution comes bundled with configuration; maintenance, troubleshooting, monitoring and log analysis tasks. These new tasks are added to the other tasks originating from the existing devices. Additional tasks diminish the amount of time spent by the administrator on each security device. There are two possible solutions for the growing workload problem of security personnel: One is "to employ more security personnel" and the other is "to make the job of the security administrators easier". Due to the scarcity of quality security personnel, it is not feasible and economically advantageous to employ more personnel. Instead, the second solution of making the tasks of the administrator easier is more applicable.

In order to deal with the difficulties of security management mentioned above, new solutions should be searched for and used in network management. The problem that this thesis study deals with is the central management of a large number and variety of security services that provide organization-wide network and information security. This study addresses two problem areas. The first problem is how to ease network management, and the second is how to better explain security issues to upper management.

### **1.3. Aim of the Study**

The aim of this study is to examine the security administration procedures, define related problem areas, and provide a convenient solution to ease the task of security administrators. The study describes the difficulties of the security administrator in two areas: managing security devices and presenting the results to upper management. Both problems have equal importance. Providing a solution that covers both issues is the goal of this thesis. A centralized security management tool that can provide a more efficient way of managing all security products is designed for this purpose.

The tool presents a framework for security administrators and security personnel to monitor their complex network devices more easily, and a means to present the results of their work in an easy-to-understand fashion to their superiors and to top management.

The Security Management System (SMS) designed in this thesis is a web-based application. Web based applications are fairly easy to code, and can run in any client environment easily. In this design, the goal is to combine performance related parameters of security devices and the network devices on a web page to reflect the overall performance of the system. The objectives are:

- To provide better monitoring capabilities,
- To present the performance parameters of the system to senior management in a user friendly manner,
- To provide a better troubleshooting capability

#### **1.4. Scope of the Study**

The research focuses on the design of a custom-made central management interface for the security administration of a medium to large sized organization. In this study, a network model that applies the concept of defense-in-depth, as described in Chapter 2, is used, and the centralized management tool is designed for this sample network.

Chapter 2 evaluates the needs for security, the threats and the countermeasures against security attacks. The importance of security investments to an organization's network, and approaches for building a secure network are explored. Besides, the tasks of a security administrator together with the difficulties of managing a network are covered in Chapter 2. In Chapter 3, network security background, security systems and current security management procedures, which are common to many organizations, are presented and the difficulties related to these procedures are examined. Chapter 4 illustrates the concept of central management with the introduction of a sample network and the detailed description of the security management system developed in this thesis. Chapter 5 evaluates the results and presents suggestions for future work.

## **CHAPTER 2**

### **LITERATURE REVIEW**

#### **2.1. The Need for Security**

The amount of digital information in the world is increasing, and this digital information is being shared throughout the world. A recently published Gartner report (Hallawell, 2004) estimated that the volume of information that organizations deal with, will be 30 times bigger in less than a decade.

The effects of information systems on daily life began to become significant in the early 90's by the introduction of one of the most exceptional inventions of the century: the Internet. Since then, the Internet became an integral part of modern human life. However, besides its impressive benefits, there are also dangers related to the Internet, most of them being about security issues. The realization of this threat was not immediate. It took sometime to comprehend the extent of the danger. Many large online companies such as Yahoo and E-bay experienced the catastrophic consequences of network attacks in the near past. Based on these consequences, the general approach to security issues has begun to mature.

Security solutions are being produced and purchased all over the world. However, according to the predictions of many security specialists, threats cannot all be eliminated; furthermore, the growth rate of security threats will be bigger than the growth of the Internet (Schneir, 2005). This emphasizes the necessity of security investments in information systems: Computers are pervasive in modern life and the Internet is an inevitable reality too, therefore proper security measures have to be in place.

In the future, conglomerates, international companies, non-governmental organizations (NGOs), governmental organizations, schools, universities, small and medium sized enterprises and even individuals will need to use information systems to some extent in order to be successful in their respective fields. In order to deal with large amounts of information, organizations will become more and more dependent on information technologies, despite the inherent shortcomings and risks such as security breaches, data theft and loss of data. Bruce Schneir (2005), Chief Technical Officer (CTO) and founder of Counterpane Internet Security, and one of the most famous security experts in the world, is certain that there is no other choice for companies but to connect their networks to the Internet and compete in the digital world.

“As risky as the Internet is, companies have no choice but to be there. The lure of new markets, new customers, new revenue sources and new business models are just so great that companies will flock to the Internet regardless of the risks.” (Schneir, 2005:2).

Competition among companies serving their customers over the Internet is very high. In order to survive, companies try to secure competitive advantages via their software, website and other information systems. Providing the best service to their customers before their competitors becomes so critical that companies often do not put enough emphasis on the security related features of the software or security testing in order not to delay their operations, even though they are aware of the threats. Companies sometimes just disregard security and do not consider it as an important issue. This negligence results in security free coding. The security-free coding of the software is a hidden threat and this threat can be covered by network security measures to some extent, but unfortunately, a full coverage of the threats is not possible.

The nature of the Internet makes it possible for anybody in the world to reach other servers, which may be located thousands of miles away, and find ways of launching network attacks. There are many types of simple attacks, which are launched with easy-to-use tools crafted by astute but malicious security experts - hackers-. Misconfigured networks are attractive targets. The motivations of hackers are various: some of them are just looking for fame, while some others are using the techniques for financial income. The realization of the malicious intentions results in attacks, abuses, theft and denial of services, resulting in millions of dollars of cost to companies.

The consequences of security incidents can be catastrophic for any company in the world. The loss of company data, money, reputation and other assets, in some cases, could even lead to bankruptcy. The risk is too big to continue without adequate investment in security.

## **2.2. Enterprise Security Management**

### **2.2.1. Common Practices**

There is a common layout and set of procedures for enterprises with a collection of security products, which is generally used when building a network. This layout is becoming a de facto standard for any security-aware company. Products such as firewalls, anti-virus software and intrusion detection/prevention systems (IDS/IPS) are present in almost every network. Besides these de facto products, new products such as anti-spyware, anti-spam software and patch management tools are becoming widespread.

### **2.2.2. Enlargement Difficulties**

As a response to the new threats and vulnerabilities, new security software and fixes are produced. If no additional precaution is taken, new vulnerabilities may be exploited and used against the companies' information systems assets. The anti-virus market is a good example for evolving security markets. When first introduced, anti-virus programs were believed to cover virus-related problems. However, in recent years, with the emergence of spam, spyware, adware and phishing as new threats, it became clear that those problem areas were not covered by the current set of security products including anti-virus programs. Solutions to the new problem areas are provided either in form of an addition to the existing products such as spam module to the anti-virus product, or in the form of a totally new program such as a content filter.

There is a production cycle in security, which starts with the discovery of security vulnerabilities. In the next step of the cycle, patches and fixes to the existing products are crafted. If the vulnerability is too complicated to be covered by a patch, then a new security device or software is produced. In the last step of the cycle, enterprises purchase new security software or update their system accordingly. The cycle restarts with the discovery of a new vulnerability and goes on in a similar way. At the end of each cycle, the enterprise network becomes crowded with new software, a security box or a new tool.

### **2.2.3. Log Handling**

All security equipments have logging capabilities. These capabilities, if handled and exploited properly, are very useful in network management, incident handling, and other networking tasks. On the other hand, it can become cumbersome

and turn out to be a burden to the administrators if enough importance is not given to log management. Matt Willard (2002) pointed out the importance of logs and log management:

“Regardless of which types of security solutions are being implemented, logging is critical to ensure their implementation is running smoothly as well to keep tabs on what is happening in an environment.” (Willard, 2002:1)

#### **2.2.4. Complexity Problem and Management Difficulties**

Networks grow as new security products, which have their own management consoles, screens, and logs to be handled by the security administrator, are added. These different devices have different locations in the network layout. Most of them are produced by different companies and are intended to be managed in a decentralized fashion. Thus, decentralized management and log handling is the default setting in many organizations. As a result, the correlations between the logs of these different systems cannot be easily checked, and the relations between them cannot be discovered easily. Sources, destinations, reasons, methods and consequences of possible intrusions cannot be detected as expected, thus the assumed benefits of the security products may not be realized.

Managing system security in an enterprise is becoming more and more complicated, since security administrators are inundated with a very high number of logs coming from different security devices such as firewalls, intrusion detection / prevention systems, anti-virus systems, routers, switches and other peripherals. All these various devices have their own management consoles, interfaces and way of presenting the logs. They all require administrators to spend time on managing the device and analyzing the logs of the device, which is a factor that may degrade the efficiency of the administrators. However, incident handling and security



management, which are the main assignments of a security administrator, requires the review of all the logs in a regular and timely fashion and quick response in order to prevent any kind of hostile network intrusion attempt, and recover from an incident as soon as possible.

Although enhanced central management devices and software are available today, they are expensive and still require a great deal of human interaction. Hyland and Sandhu (1998) discussed that every method of security management requires human presence to some degree at every security device along with manual handling and evaluation of the security logs. Nevertheless, remote monitoring and centralized management with correlation and aggregation capabilities are seen as viable solutions for network security management.

Even though these correlation and aggregation capabilities are useful, those systems are far from providing a full solution. The problem is due to several reasons such as the lack of universal standards for log generation, inadequate correlation capabilities of the software compared to the human brain, along with the price of the software. Hyland and Sandhu(1998) emphasize the lack of standards as one of the most important obstacles:

“We also believe the lack of standard definitions for managed security objects have limited more widespread, interoperable implementations.” (Hyland and Sandhu, 1998)

“Like other distributed applications, security management modules must speak a common language. “ (Hyland and Sandhu, 1998)

New software products came out recently claiming to solve the standards problem to some degree. But the price of the software is often prohibitive for many organizations. One of the new technologies emerging to solve the ‘excessive logs’

problem is a software that can analyze all the logs, aggregate and make correlations and present results in human-readable format. One of the commercial products of this kind is TriGeo's Security Information Management (SIM). In 2003, the price of this product started from \$250.000 for a medium-sized implementation (Martin, 2003).

Due to the aforementioned shortcomings, there are no widely used and accepted commercial products in security management today. Martin (2003) underlines this problem: "Despite vendor hype, management tools for secure applications are limited in capabilities and generality" (Martin, 2003). Until a consensus on common criteria and definition of standards is reached companies have to find the best solutions available in the market, or produce their own solutions to overcome the problems of distributed security systems.

## **2.3. Designing a Secure Network**

### **2.3.1. Design Goals**

"There is no such thing as 100% security." (Rosamond, 2004; Bertagnolio, 2001). Both Rosamond and Bertagnolio state that since the Internet is not completely secure, any network connected to the Internet cannot achieve total security. Besides, security is a process, not a task to be completed. Efforts on providing security must continue as long as the network is functioning and is connected to the Internet.

The main goal of designing secure networks is to manage the risks as effectively as possible, rather than eliminating all the threats (Bertagnolio, 2001). Security administrators ask six questions about the incidents: Why, Who, What, Where, Why and How. A secure network, in principle, should be designed to provide

the administrators the answers to these questions. A secure system must have all the watching, monitoring and logging capabilities (Abramson, 2001).

In one of its articles, the Microsoft tech-net web site identifies 10 immutable laws of security administration (Microsoft, 2007). One of the laws of security administration is listed as ‘the most secure network is a well-administered one’. This sentence indicates the importance of the configurations of the network. Actually most successful attacks are not executed by exploiting a flaw in the software, but by taking advantage of the misconfigurations in the network. Another important law of security administration is about the complexity of the network. It states that ‘the difficulty of defending a network is directly proportional to its complexity’. Keeping it simple, documenting every configuration change, updating security policies are all good components of successful security management.

### **2.3.2. The Concept of Defense-in-Depth**

The concept of Defense-in-Depth is a layered approach to network security. The basic definition of Defense-in-Depth is “not putting all the eggs in one basket” (Miles, 2004). This simple analogy refers to not putting all the emphasis on a single defense mechanism for the protection of a network, but relying on several different security measures in a layered approach. There is no single product in the security products market, which can completely protect networks from all the different types of threats. Applying security countermeasures in multiple layers improves the overall strength of the security. In this approach, if a security precaution fails, there is another level of protection that can prevent the attack.

Defense-in-Depth is a widely used practice for building secure networks. In this strategy, the plan is to install different security software in such a way that those

installations would provide challenges for attackers. These different security software may overlap with each other, but there should not be any gaps between the layers. An intruder has to navigate through all the measures to find the target. With all these levels of security measures and careful monitoring, the probability of launching an attack without leaving any trace decreases. Different security precautions at each level mean different technologies and diverse methods of protection to be overcome by the attacker. Scott Rasmussen (2002) discusses the issue as “The more layers, to a degree, the stronger the security and the more diversity the more comprehensive the protection”.

Nicholas Arconati (2002) discusses the requirements of an effective enterprise security architecture and positions Defense-in-Depth among the top requirements for secure enterprise.

“A strategic and effective enterprise security architecture of today needs to be based on “Defense in Depth” which is a concept used to describe layers of defense strategies. The components at each layer work in tandem to provide one cohesive security mechanism. This layered approach will also help localize the impact if one element of the mechanism is compromised” (Arconatti, 2002).

### **2.3.3. Public – Demilitarized Zone (DMZ) - Private Network Layout**

In addition to the implementation of the Defense in Depth concept, Arconatti (2002) proposes the implementation of “Tiered Networks”. This is to ensure that the most important data will be stored in the most secure segment of the network. The “Tiered Networks” approach divides the network architecture into three main segments: Public, Demilitarized Zone (DMZ), and Private. The Public-DMZ-Private setup is widely applied in many networks (Rosamond, 2004). Public is the global Internet, on which enterprise security staff do not have any control. Private is the enterprise network, where access from the Internet is prohibited. DMZ is a network

segment, which serves as a buffer zone between the public and private network segments. The servers for users outside the enterprise are located in the DMZ. Access to the DMZ is not prohibited but limited to some ports.

Since there is no complete solution for the security of the Internet, there should be a separation between the company's network and the Internet. That is why the public and private parts must exist in every network. Since there are some services that should be publicly accessible such as e-mail and web, the servers of these services must be located in between the Internet and the organization's network, which is the DMZ. Arconatti (2002) defines the segments of the approach with different terms:

- “The **Internet tier** consists of the global Internet. The enterprise security policy does not control every device on the Internet, but does enforce requirements upon these devices accessing the enterprise network.
- The **Extranet tier** consists of a protected extension of the corporate Intranet. This extension is often protected by a demilitarized zone (DMZ). In some cases, the DMZ is the extranet tier.
- The **Intranet tier** consists of the private enterprise network” (Arconatti, 2002)

In order to provide better security, some additions can be applied to the basic public-DMZ-private layout. Instead of using one DMZ, more than one DMZ can be created, and application servers can be grouped and located in those zones. By creating more than one DMZ, access control can be applied more efficiently. For example, in a complex network, three DMZs may be created: management DMZ, database DMZ and external DMZ. The management servers of security devices are located in the management DMZ, while the database servers are located in the database DMZ, and other application servers are located in the external DMZ. In this layout, additional security may be applied to database servers and access to the database DMZ can be restricted to only application servers.

## **2.4. Security Administrator Responsibilities**

### **2.4.1. Definition**

Company networks are run by administrators. Even though their tasks and areas of responsibility may overlap in some cases, they are given a specific title such as Network Administrator, Security Administrator, and Database Administrator. The security administrator is generally responsible for the application of information systems security policy in the enterprise. To achieve this goal, there are numerous tasks that must be carried out by the security administrators.

### **2.4.2. Tasks of Security Administrators**

The most important task of a security administrator is analyzing, aggregating and correlating diverse logs. Other significant tasks are investigating security incidents, providing periodic or impromptu reports to upper management, following the new developments in security, evaluating new security products and providing training for management and employees. According to Setty (2001) selecting secure passwords, keeping the systems up to date, patching, vulnerability testing and monitoring the system periodically are also among the task of security administrators.

The tasks of security administrators can be classified as daily, nightly or early morning, monthly and ad-hoc routines as shown in Table 2.1 (Michael Espinola Jr's Wiki, 2007).

Table 2.1 Tasks of a Security Administrator

<b>TYPE</b>	<b>TASK</b>
<b>Daily</b>	Review physical hardware status
	Review logs
	Review queues
	Monitor information, software, services, and status.
<b>Nightly and/or early-morning</b>	Anti-virus update
	backups
	security patching
	software updates
	rebooting
<b>Monthly and/or ad-hoc</b>	Security and penetration testing
	Load testing
	Software installation
	Troubleshooting

#### 2.4.3. Challenges of Security Administrators

In order to perform the tasks related to log management as expected, all the logs should be presented in a central station. Figure 2.1 is taken from a research conducted by SANS Institute in 2004 (Martin, 2004). The ‘Analyze’ part of the depicted procedure, shows the centralized log analysis station. Figure 2.1 urges the application of a centralized log analysis system in order to provide better means for security administrators to produce the expected results.

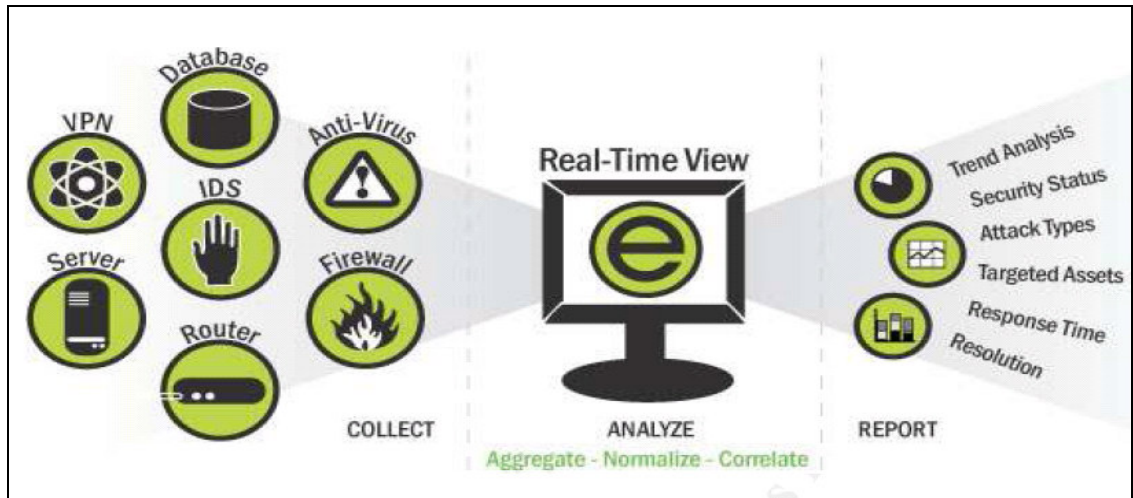


Figure 2.1 Logical Flow of Security Information Management (Martin, 2004)

Willard (2002) points out the difficulties of dealing with excessive amounts of logs manually and the consequences if logs cannot be handled properly.

“While it is easy to suggest that all logs should be looked on a weekly, if not daily basis, the amount of information commonly logged is so great and often times in a format that is difficult to understand, it becomes a tedious job that more times than not gets overlooked. As a result logs are either not reviewed at all or given a cursory review, which results in the most critical items being missed altogether” (Willard, 2002:1)

#### 2.4.4. Ways of Serving Better

In a report about Information Security Management, published by the United States General Accounting Office (US GAO, 1998), experiences gained from leading organizations are reflected. The report gives advice to Senior Security Officers about how to better serve the members of the organization and senior management. The advices are generally about establishing a reporting system for both security personnel and for other high-level managers. Table 2.2 presents the advices taken from this report.



Table 2.2      Advices to Administrators (US GAO, 1998).

No.	ADVICES TO THE ADMINISTRATORS
1.	Establish a reporting system to account for the number and type of incidents and related costs.
2.	Establish a program for testing and evaluating key areas and indicators of security effectiveness.
3.	Develop a mechanism for reporting evaluation results to key business managers and others who can act to address problems.
4.	Become an active participant in professional associations and industry discussion groups in order to keep abreast of the latest monitoring tools and techniques

The main tasks of security administrators are common in all the documents mentioned in this section. These common tasks are maintaining the security of the network, monitoring the status of the devices, examining the logs and reporting the results to upper management. These require the use of a Security Management System (SMS) such as the one designed in this thesis that can centrally present the related data about the state of the network.

## 2.5. Monitoring

### 2.5.1. The Importance of Monitoring

“The full spectrum of security embraces detection, prevention and recovery.” Terry Gray of the University of Washington said when defining security (Kvavik, R.B., et al., 2003). The first and most important phase of security in incident handling is the detection phase, since only detection can trigger the prevention mechanisms and can make the recovery easier. If detection mechanisms are not sufficient, independent of the extent of the prevention and recovery capabilities the organization has, those capabilities cannot be exploited fully and they may become obsolete. Detection mechanisms comprise a monitoring system and a correlation process. An

adequate monitoring system collects the logs and performance parameters of the security devices in the organization and presents them to the administrators in a user-friendly style. Security administrators generally carry out the correlation process with the help of security devices. Therefore, a good monitoring system is a prerequisite for the entire security of the organization, without it, other investments become useless.

Lack of monitoring is among the top reasons for security breaches and network attacks. In a survey conducted by the Educause Center for Applied Research, security administrators are asked how frequently they monitor their systems (Kvavik, R.B., et al., 2003). 68% of the participants in the survey declared that they review the logs daily, while 12% reviewed weekly. The others did not mention a period for their review. The results are not so bad but far from perfection. The main problem is about the one third of the participants who do not monitor their systems daily.

Schneir (2005) has parallel evaluations with Terry Gray (Kvavik, R.B., et al., 2003). According to Schneir, real-world security includes prevention, detection and response. Since no prevention mechanisms, especially those for networks, are perfect, there is and will always be a need for detection and response capabilities in network security. Detection capability is only present when a decent monitoring mechanism is running and staffed with apt administrators.

The Computer Emergency Response Team (CERT) of the University of Carnegie Melon, provides a detection checklist, and includes the steps for an administrator to follow in case of an intrusion. The checklist starts with the examination of the log files. (CERT, 2007).

### 2.5.2. The Need for Human Intervention

Schneir (2005) discusses the need for human intervention in security and argues that network security sensors and devices do not offer security by themselves. Software can only provide generic information; real understanding requires experts. Software can provide some alerts for administrators, but they cannot replace administrators in analysis. These alerts are only good for administrator to:

- “Analyze what the software finds suspicious,
- Delve deeper into suspicious events , determining what is really going on,
- Separate false alarms from real attacks, and
- Understand context. “ (Schneir, 2005)

Schneir (2005) insists on a defense posture, which is a combination of human, and software interaction. For him, automatic security is not enough, while the administrators cannot do anything without the help of security software either.

“The key to effective security is human intervention. Automatic security is necessarily flawed. Smart attackers bypass the security, and new attacks fool products. People are needed to recognize, and respond to, new attacks and new threats. It is a simple matter of regaining a balance of power: human minds are the attackers, so human minds need to be the defenders as well.” (Schneir, 2005)

Cisco, one of the leading manufacturers of networking equipment worldwide and a technology giant, provides a best practice guide for the implementation of network security (Cisco, 2006). In this document, Cisco emphasizes the importance of monitoring the security of the network and lists it as one of the top priorities of security administrators. It also points out the necessity of a skilled security team.

“While network monitoring often identifies a security violation, it is the security team members who do the actual troubleshooting and fixing of such a violation.” (Cisco, 2006).

In the paper, Cisco recommends that every network should have a monitoring policy for each risk areas identified in risk analysis.

“...create a monitoring policy for each area identified in your risk analysis. We recommend monitoring low-risk equipment weekly, medium-risk equipment daily, and high-risk equipment hourly. If you require more rapid detection, monitor on a shorter time frame” (Cisco, 2006).

The importance of “trigger” is mentioned in the article. Additionally, the security team members should be notified when an incident happens. This can be done via e-mail, a pop-up alert, or even with a short message or via pager.

“Lastly, your security policy should address how to notify the security team of security violations. Often, your network monitoring software will be the first to detect the violation. It should trigger a notification to the operations center, which in turn should notify the security team, using a pager if necessary.” (Cisco, 2006).

## **2.6. Incident Handling**

Monitoring by itself only gives the necessary reaction time to apply countermeasures against incidents. Since time is very important in incident handling, organizations should have a predetermined set of regulations to be applied in case of security breaches. Successive steps to recover from a security incident are also defined by Cisco (2006). The first and most important step is notifying the right person at the right time. Further steps of reaction are listed as follows:

“ The first action following the detection of an intrusion is the notification of the security team. Without a procedure in place, there will be considerable delay in getting the correct people to apply the correct response. Define a procedure in your security policy that is available 24 hours a day, 7 days a week.

- Implementing changes to prevent further access to the violation.
- Isolating the violated systems.

- Contacting the carrier or ISP in an attempt to trace the attack.
- Using recording devices to gather evidence.
- Disconnecting violated systems or the source of the violation.
- Contacting the police, or other government agencies.
- Shutting down violated systems.
- Restoring systems according to a prioritized list.
- Notifying internal managerial and legal personnel. “(Cisco, 2006).

The final step is gathering the evidences of the attack in order to determine the extent to which the system has been compromised by the attack, and to prosecute the external or internal violators.

## **2.7. Upper Management’s Involvement in Security**

### **2.7.1. Importance of Security Awareness**

According to Nicholas Arconati (2002), enterprise security is not only a technical challenge for administrators and security staff; it is a management and social problem as well. For building a secure network architecture, there should be written rules and policies in the first place. Based on these policies, security awareness and security culture can be built in the organization. For the people in the organization, it may not be easy to accept security precautions, since a new security precaution usually means giving up a user-friendly attribute of the system. However, if security awareness starts from the top and goes down to cover all the employees, than it is more acceptable by everyone.

“The creation of enterprise security architecture begins by defining an enterprise security policy that everyone in the corporation accepts and supports. This starts at the top. The CEO must endorse, support, and abide by the policy. The policy must be enforced through all levels of management on down to every user. In many cases this results in an information security user awareness program that educates the users and ensures user acceptance.” (Arconati, 2002:3).

### **2.7.2. Responsibilities of Upper Management**

The security of a network is not solely the responsibility of security administrators. Security is the task of every employee in the organization including upper management. Besides the commitment of the employees to security and their awareness level, upper management's involvement is critical to the organization's success in maintaining a secure network. Upper management's importance is due to the fact that they have the power to enforce security policies organization wide, and they command the investment decisions in the organization. The IT Governance Institute published a report in March 2006 (IT Governance Institute, 2006), to serve as guidance to the board of directors and executive managers, in which the importance of executive level involvement is mentioned as follows:

“Information security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability. Effective security requires the active involvement of executives to assess emerging threats and the organization's response to them.” (IT Governance Institute, 2006)

The report also list the security related responsibilities and tasks of senior executives. These responsibilities are about designing the network, security policy development, implementation of security, employee awareness of security, security training and education. Besides these tasks, one other security-related task that has importance is monitoring.

“ Establish monitoring measures to detect and ensure correction of security breaches, so all actual and suspected breaches are promptly identified, investigated and acted upon, and to ensure ongoing compliance with policy, standards and minimum acceptable security practices.” (IT Governance Institute, 2006)

### **2.7.3. Upper Management Commitment to Security**

The vice president and the research area director of Gartner group, William Malik, mentions senior management's responsibility and states that the integrity of the enterprise depends on senior management's commitment to information security (Lee, 2001). It should not be forgotten that, this support does not guarantee success, but lack of commitment will increase the possibility of a failure (Lee, 2001). Lee offers a way of persuading all business units including senior management by showing them the possible consequences of security breaches which may be catastrophic.

“Emphasizing the negative effects of a loss experience on the whole organization can be one way of applying pressure to motivate all business units to improve security.” (Lee, 2001)

Rosamond (2004) discusses the administrative and funding difficulties in building a secure network. He emphasizes the importance of senior management support the proficiency of the Information Technology (IT) staff.

“The main constraint (of building a secure network) would clearly be both the willingness of senior management to to allow these changes, and most importantly, having a technically proficient IT staff capable of implementation.” (Rosamond, 2004)

### **2.7.4. The Evaluation of Security Investments**

Information Security Governance, when implemented in an organization, should deliver some desired outcomes. One of the categories of outcomes is about performance management. Performance management is related to measuring, monitoring and reporting on information security processes, which can be used to

check whether the goals of security investments are reached or not. There are some metrics given in the report to be used to evaluate the performance of the system;

- “Number of incidents damaging reputation with the public
- Number of systems where security requirements are not met
- Time to grant, change and remove access privileges
- Number and type of suspected and actual access violations
- Number and type of malicious code prevented
- Number and type of security incidents
- Number and type of obsolete accounts
- Number of unauthorized IP addresses, ports and traffic types denied
- Number of access rights authorized, revoked, reset or changed“  
(IT Governance Institute, 2006).

These metrics should be presented to top-level management to allow them to evaluate the success of the security systems. This presentation can be made in forms of daily, weekly or monthly presentations or via written reports. However, one other effective and time saving way of presenting these data is via a webpage or a web based application as the one designed in this thesis. Web based applications have several advantages over written reports or presentations. These applications can get real time data and present it in a clear and understandable format to top-level managers. Implementing a web-based application gives the opportunity to upper management to monitor their security devices’ performance as and when needed.

## **2.8. Conclusion**

Computer security has tremendous importance in today’s dangerous Internet environment. In organizations, there are common practices about building a network. Applying the common practices and connecting security devices to the network is the responsibility of security administrators, however, every additional security precaution brings an extra load to the security administrator. The most important tasks of a security manager are designing a secure network, monitoring the security



incidents and logs and incident handling. However, the first thing that should be present in an organization is an organization-wide awareness about security threats and the necessity of security precautions. Top-level managers should be involved in establishing policies and should cooperate with security administrators.

The Security Management System (SMS) designed in this thesis and described in Chapter 4 is a management tool through which both security personnel and top-level managers can monitor the status of the network in a timely fashion. With the help of this system, security managers can get the triggers and see the abnormalities in the network. Top-level managers can monitor the security status of their company.

## **CHAPTER 3**

### **DETERMINATION OF REQUIREMENTS AND SECURITY MANAGEMENT**

#### **3.1. Determination of Requirements**

An important aspect of this research is to identify the difficulties of security management, and present a solution that would help overcome these difficulties to some degree. The solution aims to help administrators manage their systems more easily, and help senior management to monitor the performance of their security investments. In the second chapter, tasks, responsibilities, and difficulties of security administrators are identified through a literature search. The author of this thesis has work experience of more than three years as a security administrator in a large enterprise. The experience of the author and the literature review constitute the basis of the problem definition. Besides, unstructured interviews were held with security and network administrators of other organizations to provide input to the problem definition.

The steps of security management that an administrator should follow in order to fulfill the responsibilities are identified before going to the solution phase. General tasks and device-related specific tasks are listed. The security devices mentioned in the research are common in most secure networks. Later, the details of these tasks are examined from a security perspective and related difficulties are observed.

Senior management is generally informed about security and network performance via written reports, full of graphics tables and numbers. Since senior managers have limited time to spend on these reports, they generally do not examine them in detail. This procedure creates consequences that are not in favor of security

administrators. These consequences are examined and a better way of reporting is proposed.

Different design approaches to provide solutions to the problems can be generated. But there are concerns about the technological, time related and economic issues of the design approaches. Feasible solutions should be technologically viable, easy to code, should not take too long, and finally should not cost too much.

## **3.2. Security Management**

In enterprise networks, there are several tasks to be carried out in order to keep the network functioning. These tasks are generally about monitoring and checking certain parameters and indicators in the network: All the servers in the network should be up and functioning with their respective services, the load of the network and the amount of bandwidth consumption should be within acceptable limits, security devices should generate logs, the updates of the software and firmware should be patched in a timely fashion, system backups should be taken properly. To accomplish these tasks, there are several methods and procedures that are carried out through the use of different software and third party applications. This diversity means that the tasks are carried out in a decentralized manner. In this part of the study, network security background, security systems and current security management procedures, which are common to many organizations, are presented and the difficulties related to these procedures are examined.

### **3.2.1. Network Security Background**

Throughout the evolution of computer networks and the Internet, there is one thing that can beat the speed of this evolution: the speed of the evolution of security risks threats and attacks. To understand the reasons behind the development of security, it is necessary to look back at the history of networks and security together.

The first successful attempt to build a network in which data can travel from one end of the country to the other was initiated by the Defense Research Projects Agency (DARPA) in 1969. Initially four organizations from around the USA were selected to participate in this project. The University of California Los Angeles (UCLA), the University of California at Santa Barbara, the University of Utah and the Stanford Research Institute (SRI) were the four organizations among which a network was established. This network was called Advanced Research Projects Agency (ARPANET), which later became the Internet we know today. After those four organizations, other academic institutions, defense-related companies and governmental organizations joined the network. (Leiner, Cerf, et al., 2003)

Since the first users of this network were academics and government employees who were only interested in discovery and enhancement, security was not really a primary concern. In the 1980s, the release of the first personal computer by Apple, and later on by IBM, and the first local area network design among personal computers (PC) by Novell boost the growth of the Internet. By the late 1980s, the PC market and Local Area Networks (LAN) grew very fast. The National Science Foundation (NSF), an agency of the United States government, created a network called NSFNET. NSFNET was the successor of ARPANET. NSFNET transferred ARPANET, which was once only available to a small group of academics and government employees, to everyone who had a personal computer.

This transformation brought the issue of security. Even though, the United States government tried to take some security precautions and enhancements, these efforts were not enough to fight the security issues. In 1988, the first ever Internet attack was launched with the introduction of a computer virus. That time there were about 60,000 computers connected to the Internet (Wikipedia the Free Encyclopedia, 2007a). In the 1990s, the growth of the Internet was so tremendous that nobody had a

clear idea about its future. Today, the Internet can be seen as a worldwide infrastructure, which was not intended to be this big in the first place and which was not designed with security in mind. The main problem today is that it lacks fundamental security mechanisms and fixing this problem is not feasible.

Today, security threats are various, based on their type, source, the intention of the attacker and the amount of damage it caused. Threats can come from inside such as disgruntled employees, or from the outside by hackers. There are several types of attacks such as viruses, trojans, logic bombs, spyware, adware, e-mail attacks such as phishing. The intention of the attackers may be not too dangerous such as finding out the web surfing habits of the users (adware), or really dangerous as theft of credit card numbers or identity theft.

The difficulty is simple: there are numerous hackers whose only concern is to find out one flaw in the system or a vulnerability that can be exploited for malicious purposes. But on the other hand, security staff is not as numerous as hackers and they have a more complicated job: they must plug all the holes, find out all the vulnerabilities and come up with solutions to all the vulnerabilities before hackers find out a way to exploit them.

Ross Anderson (2001) gave a striking illustration and demonstrated this fact in his article. The example was about a hacker who has limited time and capabilities, and who can find only one bug a year in a big organization's network or in a big piece of software such as an operating system. On the other side of the example, there is a security team in the organization with adequate personnel and time to find 100,000 bugs in the same year. When we consider that the system is as complex as the Internet and the software is as complicated as Windows 2000 which can have

about 1,000,000 bugs, then the probability of the security team's discovery of the same bug as the hacker is only 10%. It means that it would take 10 years for the security team to find the same bug as the hacker, and if the hacker had found 10 bugs, then it would be nearly impossible for the security team to cover all the 10 bugs of the hacker. Moreover, it should not be forgotten that there is not only one hacker. As a result, Anderson concludes that:

“Even a very moderately resourced attacker can break anything that's at all large and complex. There is nothing that can be done to stop this, so long as there are enough different security vulnerabilities to do statistics: different testers find different bugs.”  
(Anderson, 2001)

### **3.2.2. Network Functioning and Server Status**

Networks are built by connecting client computers and servers with each other with the help of intermediate network equipments such as routers, switches and hubs. All these equipments are connected with copper or fiber-optic network cables. The full operability of a network is only possible when all the servers, computers and intermediate network devices are up and running. A sample network diagram is shown in Figure 3.1.

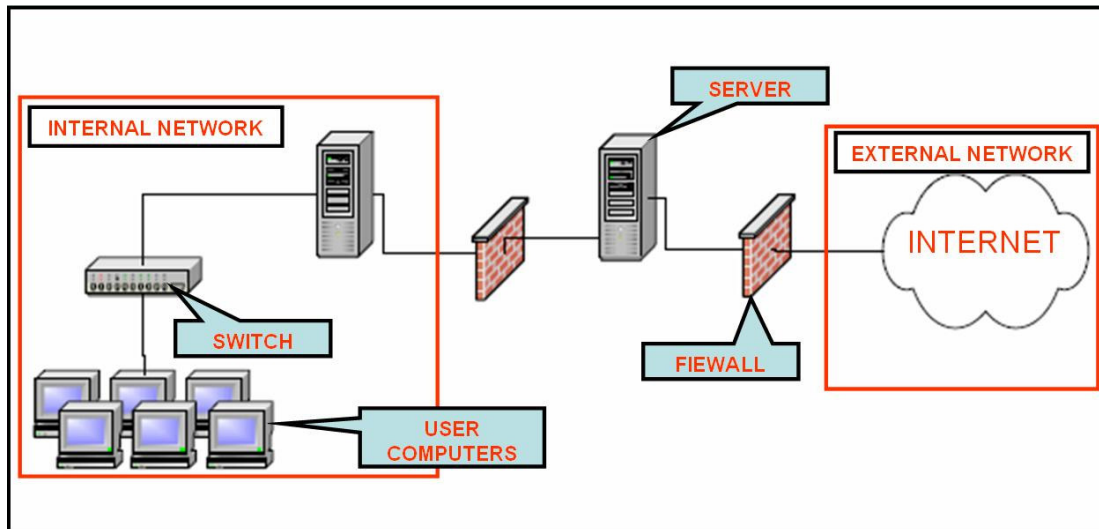


Figure 3.1 Basic Network Diagram

The introduction of the network protocol family, “Open System Interconnection (OSI) layered model” made it possible for the Internet to grow with tremendous speed. The International Organization for Standardization (ISO) began to develop the OSI model in 1977 and published its abstract model in 1980 (Zimmerman, 1980). OSI proposed the use of a layered model, which organizes the communication with its seven layers. These layers communicate with their peers on the other end of the communication and only interact with the layer above or below itself. The first layer is known as the “Physical Layer” in which the bits are transferred to the wire. The second layer is the “Data Link Layer”, while the third and fourth layers are known as “Network” and “Transport” layers respectively. The fifth, sixth and seventh layers are known as application layers in general. The names of these layers are “Session”, “Presentation” and “Application”. Since this model is abstract, it is not applied with all its layers in real life; rather it is used as a template.

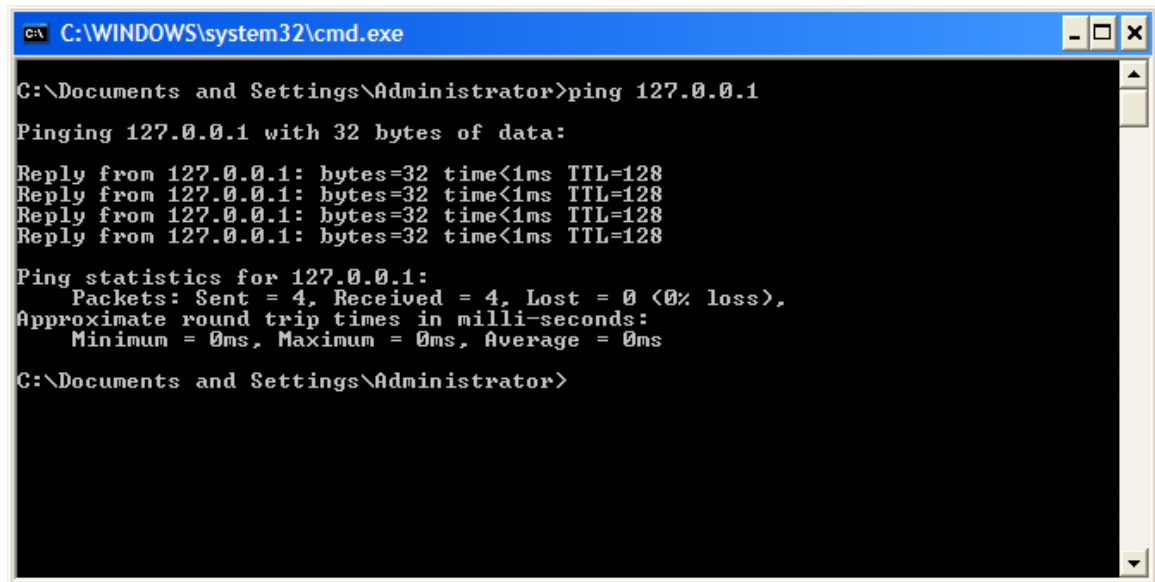
Network devices communicate with each other over network protocols. There are several protocols for every layer of Internet communication. The most popular

network protocol family is the Transmission Control Protocol over Internet Protocol (TCP/IP). The Internet runs over TCP/IP. IP makes the communication possible with the help of IP addresses, while TCP distinguishes the service applications running on a computer by using port numbers. For example; all web serves have an IP address which is known by every client computer and a service running on port 80, which is the default service port number for web servers.

### **3.2.2.1 Ping Command**

Besides the main protocols of the Internet, there are other protocols designed to control, test and maintain networks. Internet Control Message Protocol (ICMP) is introduced to help administrators check the functionality of their devices and help troubleshoot networking problems. This protocol is popular with its famous application known as “ping”. This is a tool, which was created by Mike Muuss in 1983, used to test whether a particular host is reachable across an IP network or not (Michael John Muss, 2007). This application sends out ICMP “echo request” packets to the destination IP addresses and waits for “echo response” packets. If an echo response packet is received, it indicates that the computer is up and can communicate on the IP network. Beside this basic information, ICMP response packets present other valuable information to administrators. The number of hops that the packet traveled to reach the destination (known as Time to Live-TTL), the time it took the packet to come from the destination computer to the source computer are other important information. In most networks, ping is used as the primary tool to check the functionality of a computer (Figure 3.2).



A screenshot of a Windows command prompt window. The title bar at the top reads "C:\WINDOWS\system32\cmd.exe". The command prompt shows the user at "C:\Documents and Settings\Administrator>" typing "ping 127.0.0.1". The output shows four successful replies from 127.0.0.1, each with 32 bytes, time < 1ms, and TTL=128. Below this, ping statistics are displayed: 4 packets sent, 4 received, 0% loss, and 0ms for minimum, maximum, and average round trip times.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

Figure 3.2 Demonstration of the Use of Ping Tool.

The first step of troubleshooting in networking, after checking the physical connections of the cables, generally starts with the ping command. There are several tools designed for this purpose based on the ping command.

The simplest way to check the status of a network is an executable batch file or a windows script file, which is designed to send out ping packets to all network devices and servers on a network. But tools, which can send out ping packets automatically and preset the information in more user-friendly way are more popular and widely used. A batch file is easy to create and easy to use, but it is not automated and does not have a friendly way of presenting the data. On the other hand, Graphical User Interface (GUI) tools can show the results in a more understandable fashion.

The absence of ping responses is a definite indicator for a problem related to the device, but the opposite is not fully correct. The existence of these responses does not necessarily mean that there is no problem with the device. If a device is

responding to the ping requests, it means that the device is up, running, connected to the network and does not have any routing problem.

#### **3.2.2.2 Service Status**

There are application servers in all networks, which are used to serve the clients in their respective functions. A web server serves the web content to the clients, while an exchange server keeps and delivers the clients' e-mails. For checking the availability of the service, it is not enough for these servers to respond to ping packets. They should also have their respective services up and running all the time. When an application is installed on a server, related services are also installed on that server. An exchange server should have its exchange services running in order to carry out the exchange server functions. The statuses of the services are manually checked on any Windows computer by running the *services.msc* command. The services should also be checked to make sure that the server is up, running and serving the clients (Figure 3.3).

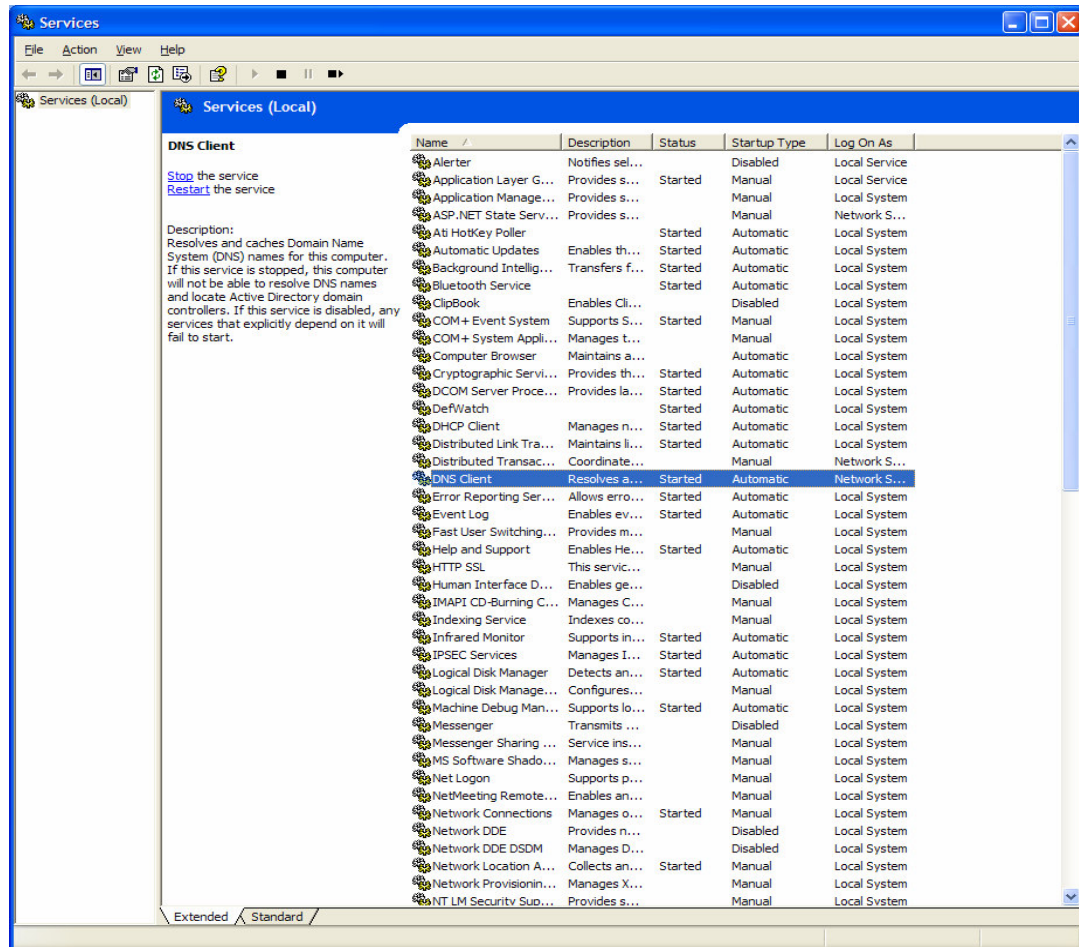


Figure 3.3 Services Control Interface in Windows Operating Systems.

### 3.2.2.3 Disk Space

Another important issue to monitor is the disk spaces of the servers. Servers are active devices that generate logs and eat up disk space quickly. If the disk space in a server is insufficient, then it cannot function as expected. There must be a way of monitoring the disk spaces of the servers in every network. There are several commercial tools that can monitor the disk spaces. These tools are run on a privileged server in the network, and they collect the data from other servers. They can present

the results in graphical formats or in tables, and also send out warning messages to the administrators.

#### **3.2.2.4 Bandwidth Usage**

There are commercial tools to monitor the bandwidth usage. These tools generate reports in graphical format. Security administrators monitor these reports in order to have an idea about the profile of the network. This profile is very important for detecting abnormal and suspicious activities in the network. If any deviation from the normal profile occurs, this should be seen as a sign for an attack and other parameters should be checked accordingly.

#### **3.2.3. Firewalls**

In today's world, most businesses, whether they are small or large, believe that for competing with other companies they should have access to the Internet. For having the privilege of Internet access, they must deal with security issues. In response to the security risks and the demands of companies, a whole industry has emerged to meet the security needs of the companies that want to have Internet connection, but stay away from the risks of the connection, and maintain the confidentiality, integrity and availability of their information assets. This industry is actually built and revolves around Firewalls. (Cisco Systems, 2002)

Firewall is among the first security measures introduced to prevent threats. During the first years of the Internet, most probably nobody was expecting that it would grow rapidly and become a very important part of daily lives, and that security would become an important issue as it is today. Once networks began growing and the Internet became widely used, threats to the security of networks and people's

concern about security and their awareness also became apparent. The need to apply some restrictions and set some barriers to anonymous users was the driving force behind the invention of firewalls. The idea of firewall is identical to the real world checkpoints. It is a gateway for company networks; same as the real life checkpoints that are used to control the access to company buildings, campuses and other important places.

The firewall technology emerged in the late 1980's when the Internet was very new, as described by Ingham and Forrest (2002). First generation firewalls were academically introduced in 1988 by Digital Equipment Corporation (DEC), and at that time they were known as packet filters. Second generation firewalls, known as stateful filters, were introduced by three colleagues from AT&T Bell Laboratories, Dave Presetto, Howard Trickey, and Kshitij Nigam. The idea behind the stateful firewall is to keep track of packets which are part of an ongoing connection. Third generation firewalls are known as application layer firewalls. Publications by Gene Spafford of Purdue University, Bill Cheswick at AT&T Laboratories and Marcus Ranum described the third generation firewall. This new technology is also known as application layer firewall or proxy based firewall. These firewalls are designed to understand certain applications and protocols. They can prevent unwanted protocols which are embedded in standard protocols. In 1994, an Israeli company, Checkpoint, introduced the first firewall with a GUI interface, which provides users an easy-to-use interface with colored icons, drag and drop options. Kernel proxy firewalls are the last generation firewalls, introduced by Scott Wigel in 1996. The first commercial product was released in 1997 by Cisco.

As introduced in the second chapter, secure networks generally isolate their internal networks from the outside world, but they create an intermediate zone, known as DMZ, to place their servers, which serve the clients outside the internal

network. DMZ's are created by the help of firewalls. Firewalls are physical devices with more than one interface. DMZ switches are attached to these interfaces and a local network is created by the help of these switches. Security of DMZ's are carried out by the help of the rules applied by the firewall.

The basic task of the firewall is to control traffic between computer networks from different trust zones. It provides a single point of defense between two networks. It protects one network from the other. (Cisco Systems, 2002) Firewall controls the accession requests and grants permission to go inside if the source of the request is in the rule table. Firewalls, beginning from the first and primitive ones, are rule based devices and are capable of filtering at layer three and four, that are known as IP and TCP layers respectively. Rules are created based on the parameters of a network packet: source and destination IP addresses and port numbers. The order of the firewall rules is important since firewalls check the packets with the rules in a sequential order. In general, the final rule of most firewalls is always a "default deny" rule. All the accession requests are tested against the rules one by one, if any match occurs between the attempt and the rule, the request is permitted, but if the attempt does not match any rule, than the final "default deny" rule applies, and the attempt is denied. Security administrators are responsible for creating rules. Proper configuration of firewalls requires skill from security administrators. Small mistakes in configuration can make firewalls worthless as a security tool.

Another important task of the firewall is that it keeps track of every single accession attempt whether it is permitted or denied. Thus, the amount of firewall logs is huge. These logs are very important for troubleshooting and incident handling purposes. There are two main types of firewalls; one of them is pure software solution, while the other is a solution of hardware and software combination. For software-only solutions, logs are generally stored on the server it runs, but for

hardware-software combination devices, the logs are stored in a remote log server. Many of the commercial firewalls come with a graphical tool for viewing the logs (Checkpoint, Juniper), however free and open source firewalls only store the logs in text format. Examining the text format logs is not an easy task. For this purpose, there are third party freeware or commercial tools for viewing the logs. It is extremely important to have a functional tool to view the logs, since security administrators must sort, filter and search for specific logs during their troubleshooting and incident handling tasks.

The performance parameters of firewalls are good indicators of the performance of the network itself. Since all the traffic coming from both inside and outside goes through the firewall, firewalls are the choke points of the networks. Any problem related to the firewall is vital for the network. Due to the heavy traffic passing over the firewall, the load is generally a good indicator for something abnormal. In the mind of any security administrator, who checks the load of the firewall and other devices daily, a profile is formed. This profile is about the load of the firewall during workdays, weekends, during the work hours, in the mornings and so forth. Security administrators know the approximate load at any time during the day. If something other than the expected load is observed on a firewall, the security administrator must take it as an indicator to make inquiries about possible attacks.

In some organizations, firewalls are unfortunately used as a “fire and forget” type of tool. Many administrators only interact with the firewall when they need to create a new rule, or need to check out the logs in case of a problem. Other than this, firewalls run by themselves. It is extremely important from the security management perspective that the logs and loads of the firewalls be monitored in real time.

### **3.2.4. Intrusion Detection / Prevention Systems (IDS/IPS)**

In the near past, it was believed that firewalls were a panacea to all the security problems of networks. It was believed that if a network is protected by a firewall then there is nothing to worry about the firewall is capable of preventing attacks. However, it was realized that the overall solution was not that simple. Even inside the legitimate and permitted traffic, hackers are capable of embedding malicious code to circumvent security systems. So the need for analyzing the legitimate traffic became an immediate security need. At this time, Intrusion Detection Systems (IDS) were introduced.

IDSs have been around for more than 20 years. The intrusion detection idea was first born with the article of James Anderson in 1980. Anderson discussed that important information about misuse and specific user activities can be found in the audit trails. There is an extreme value in analyzing these logs for understanding the user behaviors and misuses. The idea of “detecting the misuse” triggered improvements in auditing. The efforts of developing the technology mostly came from the United States Military. The first commercial product was introduced in 1997 by a security company called ISS. Their product was “RealSecure”. After that, there have been several players in the market with different products.

IDSs are designed to detect malicious network traffic that firewalls cannot detect. Intrusion Detection Systems deal with the network traffic flowing on a wire between the connected computers. These devices are passive in nature, since they only sniff the packets, and are transparent to both receiving and sending parties. They are composed of several components. There are sensors that collect the security data and generate the events, a console to monitor the events and control the sensors, and a



central engine to look for alerts among the logs by comparing them with the signatures and other detection methods.

These systems are passive systems, which do not take action against intruders. IDS analyze the traffic and create an alarm or a warning when a match is found with the signatures or an anomaly is detected. Once the packet is captured, the IDS engine applies techniques to analyze the traffic. The most common of these techniques is comparing the packet to a list of attack signatures. It is similar to comparing a fingerprint to a list of criminals' records. Other techniques include anomaly detection which is based on detecting deviations from the normal profile of the network and which does not need any signatures to do this. Anomaly detections provide a protection for the period between the discovery of the vulnerability and the release of the signature for an attack related to this vulnerability.

Being a passive system and the result of several other shortcomings, signature based IDS are becoming obsolete. The time gap between the discovery of the vulnerabilities, exploits and signatures is getting smaller. The number of logs is increasing with the addition of each new signature. There have been new additions to the basic signature-based IDS including the final one of prevention capability. These capabilities changed the name of the product to Intrusion Prevention Systems (IPS). IPS is capable of blocking and resetting the traffic if that traffic matches the criteria of being malicious. To accomplish this goal, IPS functions as an active component rather than being a passive device. All the traffic in that specific network passes through the IPS, similar to the firewall.

IPSs use traffic analysis and anomaly detection engines in order to reduce the reliance on signatures and avoid the number of false-positives. An average IDS runs

with about 6000 signatures. IPSs generally are configured to block about 25 to 50 signatures. Other traffic passes through the IPS in monitoring mode. So blocking the most frequent and well-known attacks by IPS and leaving others to be monitored by IDS is a good solution.

Despite the new capabilities of IDS/IPSs such as anomaly detection and protocol analysis, attack signatures are still very important for these devices. The difficulty of maintaining an up-to-date database of these signatures is a very big obstacle for both vendors and users. A signature must be added to the database for a new vulnerability and attack pattern, otherwise the system becomes obsolete.

Another important difficulty is the amount of logs that a security administrator should review. There is a dilemma between the number of the signatures and the amount of logs. For IDS to function properly there must be attack signatures to cover nearly all kinds of attacks. These signatures must be activated, and the traffic monitored. However, the size of the logs grows with the number of signatures. A security administrator has to go through all the logs and eliminate the false-positives to find out the real attacks. This process is cumbersome. Moreover, reviewing the logs is a reactive solution rather than being a proactive solution. In order to use the IDSs as proactive measure, the logs must be monitored in real time. Monitoring the logs in real time requires adequate dedicated personnel. IPSs do not require as much monitoring as IDSs, however the amount of false positives in IPS must be dealt with, since IPSs, different from IDSs, reset and block the suspicious traffic.

Dedicated personnel must monitor the logs of the IDS/IPS and try to find out real attacks by eliminating the false-positives. Similar to firewalls, security

administrator must build a profile of the system from the IDS/IPS point of view. The number of attack logs, either real or false positive, has to be known by the administrator for every day of the week and every hour of the day. If a deviation from the profile is detected, it should be seen as a trigger to search for possible attacks.

### **3.2.5. Anti-Virus Software**

Fred Cohen is an American computer scientist who is best known as the inventor of the first computer virus (Cohen, 1984). Since he was an academic, his intention was not malicious; rather he was testing computer security. As the inventor of computer viruses, Cohen defines virus as “a program that can infect other programs by modifying them to include a, possibly evolved, version of itself” (Cohen, 1984). There are numerous viruses, which can perform different functions from humorous simple jokes to malicious activities such as destroying all the data on the computer hard drive.

The “brain” was the first successful malicious virus crafted by a Pakistani computer science student in the 1980’s. The introduction of the first Anti-virus software dates back to late 1980’s (Wikipedia the Free Encyclopedia, 2007b). These products are computer software, which are designed to identify and eliminate computer viruses, and other similar malicious software known as malware. Similar to IDS/IPS, there are two methods of achieving this goal. The first method is examining files and looking for known virus matches with definition files. This method is known as signature-based virus detection. The second method is based on identifying the suspicious, abnormal behavior of the computers. The idea is to detect computer viruses even before a signature is created for that particular virus.

Most of the commercial anti-virus software use both methods. Signature based solutions can guarantee the detection of the virus, if the signature of that virus is in the database. The most important issue with this method is maintaining an up to date virus database. Anti-virus software companies should have a highly qualified group of people to look for vulnerabilities, create signatures, and there should be an easy method for updating the client software through the Internet. Anomaly detection and detection of suspicious behavior cannot guarantee anything, but it offers something that signature based protection cannot match. The idea is to catch a virus that is fairly new and none of the security personnel know about it. By this method the virus is detected and its activities are blocked.

Anti-virus software, similar to other security precautions needs close monitoring, reviewing of the logs, and updating. Anti-virus software generally produce statistical logs such as the number of the files examined, the number of infected files, the type of the virus and the time of detection. Anti-virus programs can be installed on desktops for PC protection, on exchange servers for e-mail protection and on gateways for web traffic protection. With the help of statistical logs, administrators can have a general idea of the network traffic and e-mail traffic. For example; on an e-mail exchange anti-virus program, there are several options that can be activated for detecting malicious activities. After a configuration is set, anti-virus software begins to block certain e-mails. Hourly, daily and weekly statistics generally give an idea about the profile of the organization's e-mail traffic. Checking out these statistics gives an indication to the administrator as to whether there is a new spread of virus or not. In anti-virus precautions, early detection plays a key role. Reviewing the logs and monitoring real-time virus activities gives the opportunity for early detection.

Another important issue about anti-virus software is updates. As a common saying in the security world: “An out of date virus scanner is only marginally better than no virus scanner at all” ([www.microsoft.com](http://www.microsoft.com)). Virus updates are generally distributed on a daily basis, but sometimes there are situations where an update has to be distributed immediately. Administrators must carefully follow the updates.

### **3.2.6. Updates**

In today’s world, technology is evolving at an enormous speed so that; software becomes out of date very quickly. Out of date software lacks the new functionalities and also suffers from security vulnerabilities. Updates are vital for the security of the system. Many software companies publish their updates on their websites and also configure their software to check the status of the updates periodically. For Windows systems, Microsoft has developed unique software for maintaining the update procedure. The software is known as Windows System Update Server (WSUS). With the help of this software, an administrator can download the updates and deliver them to the client computers and servers. The main advantage of WSUS is its central management of the whole process. Automated installation instructions can be configured according to the type and the importance of the update. The receiving end of the updates such as client computers, servers or a specific computer group can be designated for an update to be installed.

WSUS is software that is installed on a Windows server. After the installation, it requires data about the other computers on the network. After detecting the computers, WSUS learns about the version of the OS on the computers and later on it learns about the updates on that computer. WSUS, at the same time, downloads all the available updates from the Microsoft web site. The final process of WSUS is to match the needs of the computers and the available updates. It presents the needs of

all computers one by one and also presents the number of the computers an update should be installed on. A web-based interface, which can be reached from any computer in the network, is used for configuration and monitoring purposes. The administrator is given the opportunity to configure the time, the receiving computers and the updates to be installed. The client computers and servers are also configured accordingly to take the updates from the WSUS server and install them (Figure 3.4).

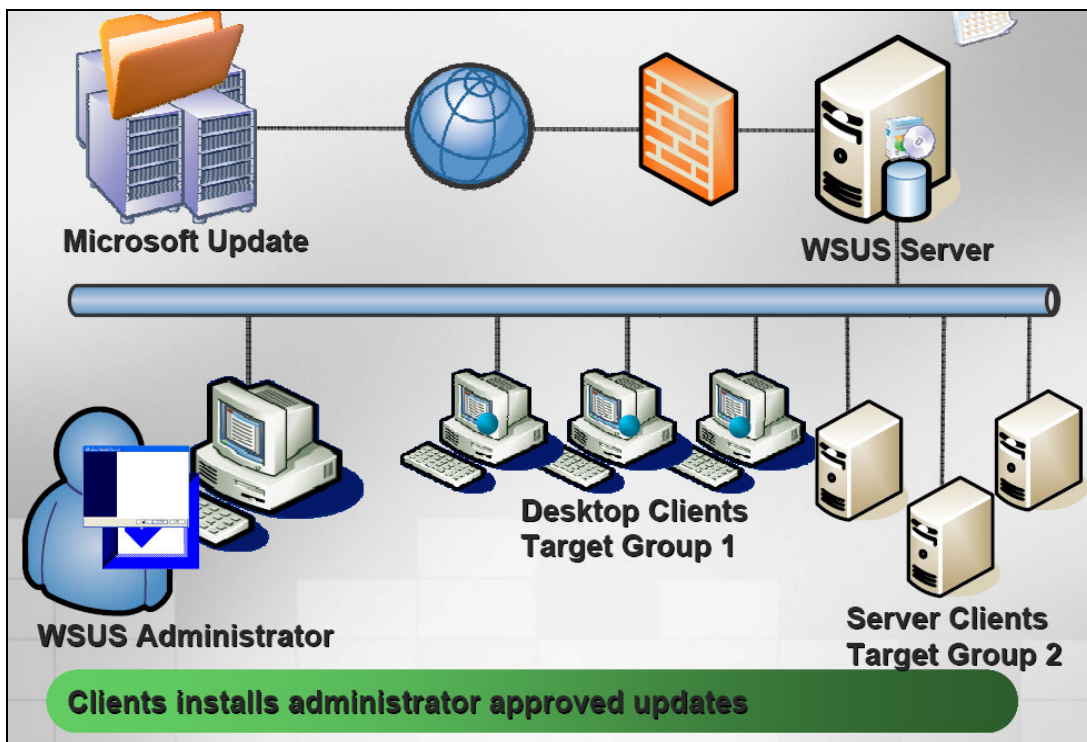


Figure 3.4 WSUS installation in a network (Koch, 2005)

By monitoring the installation of the updates, an administrator can understand the state of the whole system at a glance. The computers which cannot be updated by WSUS can be handled manually by the administrator. The administrator can disable a computer remotely if he sees a danger for the connection of that specific computer. Per computer and per update reports, summary status and alerts are available through WSUS.

### **3.3. Reports**

Security devices generally come with reporting tools. These tools provide capabilities for generating routine reports such as hourly, daily, weekly or monthly, and on-demand reports which are the reports that an administrator generates when he needs the report. There are ways of generating reports, the more common one being, generating through the reporting module interface. For this, security administrators must use the reporting module's interface, select the report and run it. The report can be viewed on the console or it can be saved in well-known formats such as a PDF file or a spreadsheet. For some security devices, security administrators can use the configuration options to have the reports sent out to administrators or other users via e-mail.

The content of the reports are generally predefined for most security tools. The reporting modules come with some default reports and unfortunately most of the time additional reports are hard to configure. Besides this difficulty, most reports are too technical to be understood by anybody other than a security administrator.

For an administrator, it is easy to understand the report, but for presenting it to upper management, the security administrator usually prints out the report and presents the paper-based version to senior management in person. This method is helpful, since there are several security related issues in the reports that only an administrator can explain. However, this procedure is painful for both sides. Senior management feel obliged to read the report that an administrator spent time to prepare, but many of the data in the report is not understandable. On the other hand, it is difficult for the security administrator to prepare a report that is easier to understand. The security administrator spends much time on preparing the reports by combining the outputs of several security devices. There is also time spent on explaining the data on the report to senior management.

Detailed explanation of the security reports to senior management is extremely important. If the necessity of the security devices and the results of its usage are not mentioned in a proper and understandable way, senior management may not realize the importance of security investments and could blame the security department in case of any incident. In order to have the support of senior management, security administrators should present the performance of the security devices to them and show that the investment in security is not worthless, and the devices are protecting the company's information systems.



## CHAPTER 4

### DESIGN OF THE SECURITY MANAGEMENT SYSTEM

#### 4.1. Introduction

The Security Management System (SMS) is a custom-made central management tool developed to overcome the problems described in Chapter 3. SMS is not the final product, rather it is a template. This template can be used to create tailored software for different networks. SMS can also be modified in case of any changes or additions of new security devices to the network. The SMS model is presented in Figure 4.1.

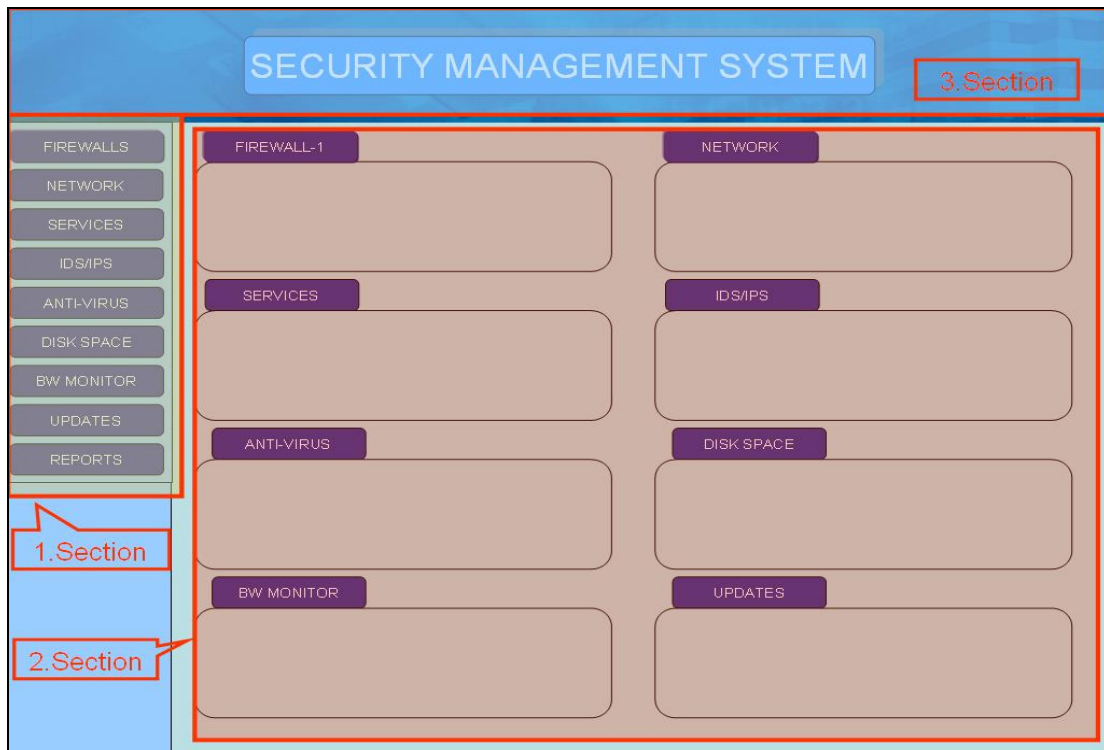


Figure 4.1 Security Management System Model and the Sections of the SMS Main Page.

The Security Management System (SMS) is designed as a web-based application, since web based applications are easy for clients to reach with a web browser, and allow the display of information in different formats such as graphics, tables or plain text to users. One other convenience of web-based applications is that they do not require any client software to be installed on users' computers for display purposes, other than the availability of a web browser such as Internet Explorer or Firefox. There are also some security benefits of web-based applications compared to others: For any application other than web services, a new network port should be opened on the server and access should be granted to those who will reach that server for that application. Web servers run on port 80, and it is generally open in most servers and also open for all user computers.

The main aim in generating the SMS model is to have a web-based application, which is easy to design and configure. Another design goal is to have an application, which provides easy access and monitoring capabilities from any computer connected to the organization's network. Since SMS will handle classified and critical information, web security precautions such as access control mechanisms (username/password, certificate, etc) or web communication mechanisms such as Secure Socket Layer (SSL) must be applied.

SMS is designed to gather all the critical performance indicators of the security devices as well as the indicators related to the overall network functionality. The design of the SMS web pages and the contents of those web pages may change from network to network. However, the main page of the different SMSs will be similar to one another since the main page is designed to present the most important indicators for all the devices. The main page of has three major sections. These sections are shown in Figure 4.1.

The first section is on the left of the page, and contains links to the web pages of the security devices. Those web pages are designed to contain detailed information pertaining to that particular security tool. Only the summary of the information presented in the web page of that device, or the most important performance indicator of the device is presented in the second section of the main page. Whenever additional information is needed, the viewers' can choose the link on the first section and reach the related pages of the SMS, where detailed information is available. In the second section of the main page, the specific performance indicators of the devices are presented in boxes. The boxes are hyperlinked to the related web pages as well as the links in the first section. The third section of the web page is reserved for the title of the system. This section is located at the top of the page. A company logo or any other related information could also be added to the title section.

#### **4.2. Model Network**

SMS is a proposed model; it is not fully implemented and tested in a running network. In order to demonstrate the functionality and design of the SMS, a sample network model is used throughout this study. The model network used in this study, contains the security tools and capabilities, which are common in many medium-size networks. The sample network has a two-firewalled layout. The Defense-in-Depth approach is used in the design of the network. The sample network layout is presented in Figure 4.2.

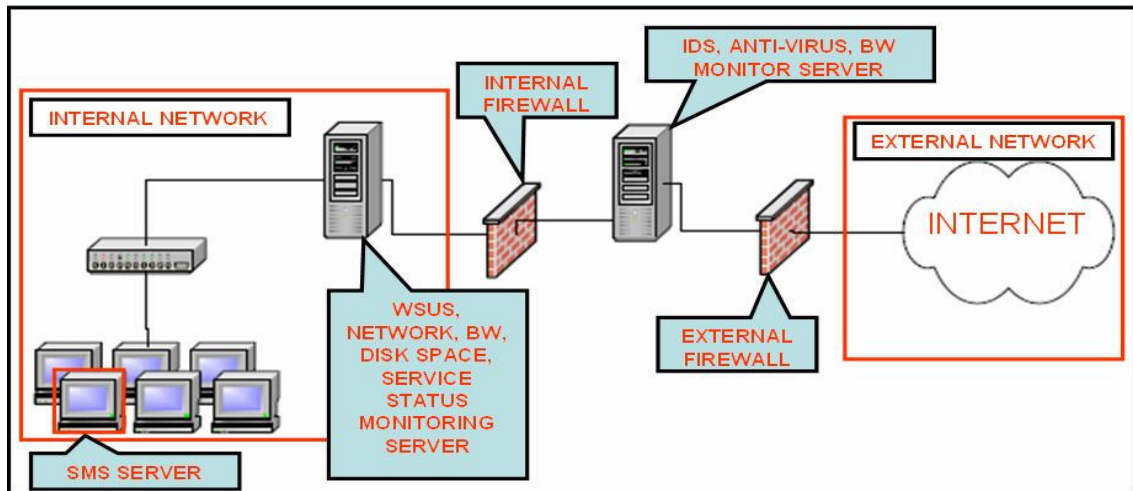


Figure 4.2 Sample Network Layout.

In the model network, there are two firewalls, one IDS, an anti-virus software for both web and e-mail protection. In addition to the security devices, there are also both commercial and free tools for bandwidth monitoring, server monitoring, network monitoring and disk space monitoring. The company also runs a server for managing the Windows updates.

Any organization, running a network similar to the sample network model, has a wide variety of options for choosing security software. In each segment of the security software market, there is competition among many security products. For this study, a security software from each product market is selected to be used in the sample network model. These selected software and their selection criteria are presented in the following sections.

#### 4.2.1. Firewall

In the sample network, there are two firewalls. These firewalls are named as internal and external firewalls according to the places they are located in the sample

network. In two-firewalled networks, the best practice is always to select different software as internal and external firewalls. The goal of selecting different firewalls is to compensate the potential shortcomings of the firewalls. For this study, Checkpoint's NGX is selected as the internal firewall and Juniper's Netscreen 500 is selected as the external firewall. Checkpoint firewall is a software-based firewall, which can be installed on any hardware such as Intel based computers and special design servers such as Nokia IP. In the sample network, the checkpoint firewall is installed on Nokia IP 350. Netscreen 500 is a hardware and software combination firewall. Checkpoint Firewalls are managed via a remote management tool called *SmartConsole*, while Netscreen Firewalls are managed via both a web interface and a remote management tool called Netscreen Security Manager (NSM).

#### **4.2.2. Intrusion Detection System (IDS)**

Intrusion detection systems (IDS) are passive in nature. An IDS is attached to a network and the network traffic passing through the network is mirrored and sent to the IDS. The IDS analyzes the traffic that has been routed to its sensors. Similar to other segments of the security products, The IDS market also has a very competitive environment. In addition to the commercial products, there are also free IDS options such as Snort. Internet Security Systems (ISS) RealSecure is one of the most popular commercial IDS products in the world. In this study, ISS's RealSecure Siteprotector is selected to be used as the IDS of the network. Siteprotector is configured to monitor the traffic coming from both inside and outside. Siteprotector sensors and the management console server are located in between the two firewalls.

#### **4.2.3. Anti-Virus Software**

Anti-virus software companies produce products for both network traffic protection and e-mail traffic protection. These two types of traffic are the most common sources of virus infection in any organization's network. In this study, Aladdin's E-safe Gateway and E-safe Mail are used as Anti-virus software. E-safe gateway is installed on a server in which all the inside and outside traffic passes through. E-safe mail works with the e-mail servers. This server checks the e-mails coming in to and going out from the e-mail servers. In this sample network, both anti-virus servers are located in the Demilitarized Zone (DMZ), between the two firewalls.

#### **4.2.4. Update Monitoring**

Common to many organizations, the sample network in this study runs different flavors of Microsoft's Windows operating systems. The updates of these operating systems are managed by specific software, solely created for this purpose. This software is Windows Systems Update Service (WSUS). This service is installed in a server in the internal network and managed by a web-based interface. By the installation of this server, Windows systems in the organization's network do not congest the organization's network connection bandwidth for updating. WSUS plays an intermediary role and acts like a proxy server. It downloads the updates and distributes them to the client computers. In the sample network, WSUS server is located in the internal network zone.

#### **4.2.5. Network Monitoring**

For network monitoring, tools including custom-made ones can be used. Since it does not require complicated tasks, any tool that can send out ping messages and check out the status of the networks can be used. In this thesis, Computer Associates' SLM (Service Level Management) software is used for network monitoring.

#### **4.2.6. Service Status Monitoring**

For this purpose, no commercial product is used in this study. The tool developed in this study is custom made for the model network. It checks out the statuses of the services which should run in order for the servers to perform their dedicated tasks. This software does not require a dedicated server but the server it is installed on should run a web service to display the results to the users. The software is installed on a server in the internal network.

#### **4.2.7. Disk Space Monitoring**

In this study, a custom disk space monitoring tool is developed for the model network. It checks out the disk space statuses of the servers and exhibits the results in graphical format through a web page. It does not need a dedicated server to run. The software can be installed on a shared server, but that server should run a web service to present the results. The software is installed on the same server as the Service Status Monitoring Software.

#### **4.2.8. Bandwidth Monitoring**

There are both free and commercial tools for bandwidth monitoring purposes. In this study, Softpedia's bandwidth monitoring software is selected. The sole purpose of the tool is to monitor and present the BW usage rates of the users in the organization in a graphical format. The tool should run on a server on which all the network traffic passes through. A server can be solely dedicated to this tool or it can be shared with other software. In this study, the server, which hosts the service status monitoring software and the disk space monitoring software is also used for the bandwidth monitoring software.

#### **4.3. System Configuration**

The SMS should be installed on a privileged server in the organization's network and the SMS server should be granted rights to access the servers of other security devices in order to capture the necessary data and display them. After the data is captured from the servers, they are processed and exhibited to the users in a more friendly and centralized way.

The hardware of the SMS server only needs to run the web service. The server reaches other servers, transfers data from those servers and runs a web service for presenting these data. Since there will not be many users of this server other than security administrators and top-level managers, there is no need to have an expensive and powerful server for SMS.

The operating system (OS) of the server is not a very critical factor. The OS can be either a Windows operating system flavor such as Windows 2003 or a Unix-



based operating system such as Sun Solaris or any Linux flavor such as Redhat Linux or Suse Linux. The distinguishing parameters about the OS selection are the licensing expenses and the expertise of the administrators on that particular OS that is chosen for SMS. One other important issue about the web servers is the web service software that would run on the server. The web service on a server is generally either Windows Internet Information Services (IIS) or Apache Tomcat depending on the Operating System on the server. Windows IIS only runs on Windows OSs, but Apache Tomcat, which is the most common web service in the world, can run in both Unix-based and Windows OSs. But the performance is better when Apache Tomcat can run on Unix-based OSs and Windows IIS runs on Windows OSs. However, when the case is the ease of use and the expertise of the administrators, Windows IIS and Windows OS are preferred over others. In this study, the selection is a Windows Server 2003 with IIS installed on it.

#### **4.4. Security Management System (SMS)**

##### **4.4.1. Design Goals of SMS**

The Security Management System is designed to be modular. It can be tailored for any organization that will use the system. For the model network of this study, SMS is intended to cover all the security devices mentioned in the previous paragraphs, which are present in the sample network. The web site is designed to have a main page and one page for each device: a web page for each firewall, IDS, WSUS, anti-virus software, disk space monitoring, bandwidth monitoring, network monitoring and service monitoring. There is also a web page in which reports of the devices are stored and presented. The main page displays the most important and significant performance parameters of the security devices, while the device specific web pages presents more detailed information about that particular security device. Main page is shown in Figure 4.3.

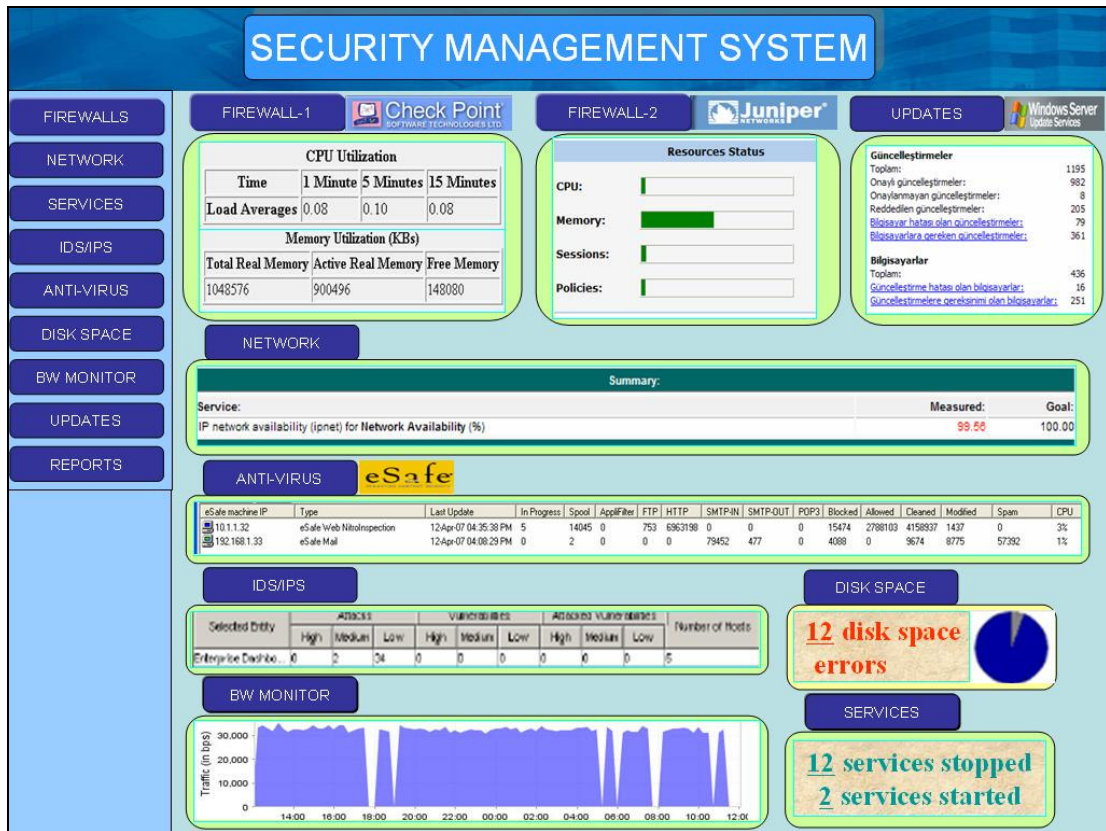


Figure 4.3 Main Page of SMS

In general, most security devices have their own ways of presenting their performance parameters and status. Some of them have web-based applications and others have their own tools. The idea behind SMS is to capture the most important and significant performance parameters of the security devices and present them together in an easy-to-understand and user-friendly web page. For this purpose, SMS server has the privilege to reach out the servers and capture the data from those servers.

Upper management can easily monitor the security status of the organizations network by the help of SMS. The graphics and the tables on the main page are a brief summary of all the security devices in the organization's network and also a way of

justifying their investment in security measures. Only by viewing the main page, upper management can monitor the real-time performance of the security devices and can comprehend how the organization benefited from the investment in security.

#### **4.4.2. Organization of the Main Page of SMS**

The layout of the main page is no different from the general scheme of the SMS. As for all the SMS pages, the second section of the main page is the most important part. When users are on the main page, they can reach the device-specific web pages of SMS when they click on either the boxes with names written on them in the first section, or the summary boxes in the second section. When users visit any page other than the main page, a ‘main page’ icon will appear in the first section, which will bring them back to the main page when clicked on. Each page focuses on a specific security device. The detailed information about the security device is presented in the form of graphics and tables. The layout and detailed explanation of the pages are presented in the upcoming sections of this chapter.

From a security perspective, there should be an access control mechanism to prevent unauthorized personnel to access the web pages and see the data on the web pages, which contain critical or classified material. Since web pages of SMS contain crucial information about the health of the network, an access control mechanism is compulsory. There are various kinds access control mechanisms such as username/password, certificate, biometric, and smart card. Most common and the simplest of access control mechanisms is the use of username and password combination. For the security of SMS, an access control mechanism at least as secure as username/password should be activated.

#### **4.4.3. Internal Firewall**

Internal Firewall is the device that connects the internal network to the DMZs and the Internet. Performance parameters of this device mainly give information about the activities of the internal users. Contrary to the common belief that the attacks generally originate from the Internet, most of the attacks (60-80%) originate from the internal users. These users sometimes have malicious intentions but most of the time they are only naive. The internal firewall is extremely important for security perimeter defense. It is the last defense mechanism in the defense-in-depth strategy for the attacks coming from the Internet.

In the model network, internal firewall is Checkpoint NGX. It is installed on Nokia IP 350 hardware. Performance parameters of the firewall are organized in two groups: one is the hardware performance of Nokia IP 350 and the other is the firewall performance of Checkpoint FW. In the SMS web page of the internal firewall, both Nokia IP and Checkpoint FW performance parameters are presented. The SMS web page of the Internal Firewall is presented in Figure 4.4.

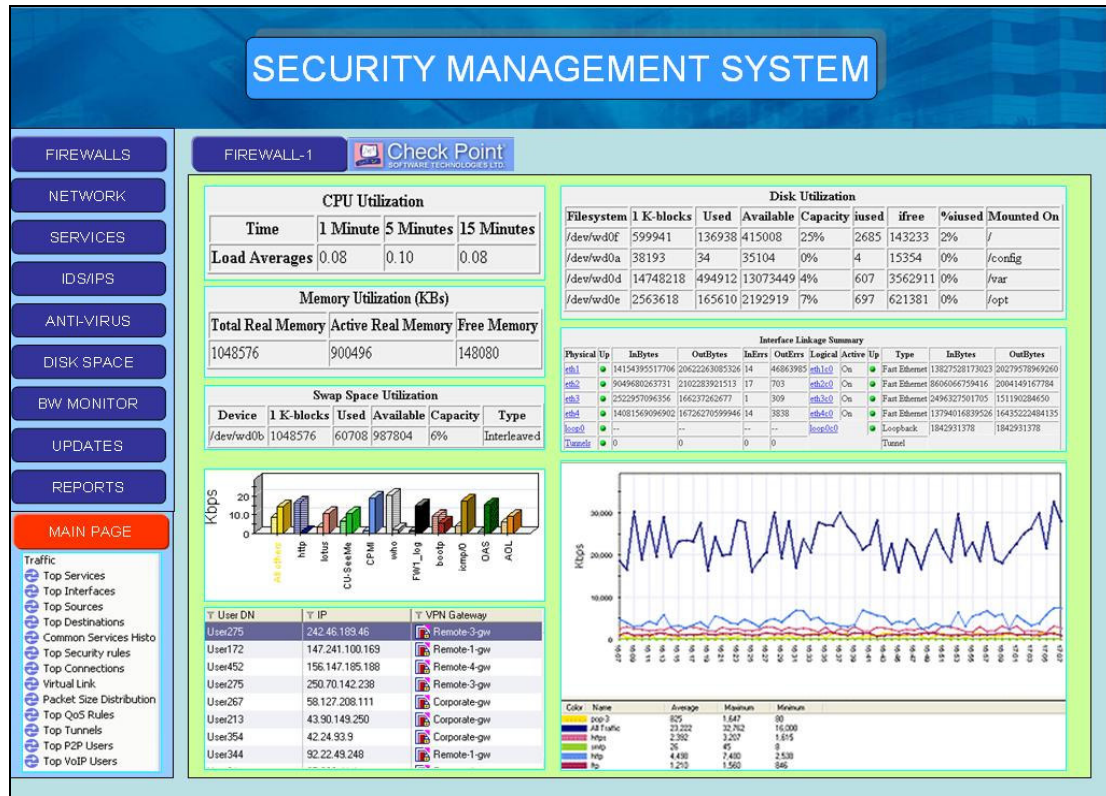


Figure 4.4 Web page of the Internal Firewall

There are two methods of managing Nokia IP devices: one is through a web page and the other is through a command line tool with Secure Shell (SSH) connection. The configuration and monitoring web site of Nokia IP devices comprise several web pages related to performance monitoring, configuration and management. These pages present the performance indicators in the forms of charts, graphics and tables. In the SMS web page of the Internal FW, some of the most significant Nokia IP performance indicators such as Central Processing Unit (CPU) utilization rates, memory utilization rates, disk space utilization rates and summary information about the network interfaces are selected and displayed. These performance indicators are selected based on their simplicity and degree of importance.

For any hardware, the most important performance parameters are related to disk utilization and CPU usage rates, therefore the graphics about the CPU and disk utilization are selected and presented on the Internal FW web page. Since this Nokia IP hardware hosts a firewall software, the performance parameters of the network interfaces are also as critical as the disk utilization and CPU usage rates to the overall device performance. The table on the web page displays the status of the interfaces with the total numbers of successful and faulty input and output packets. There are indicators for the statuses of the interfaces: green light for 'up' and red light for 'down'.

Checkpoint Firewall is managed through SmartConsole, which is a software tool installed on user computers. In order to run SmartConsole, an authenticated FW user should log on. These remote users of the firewall should be defined on the main control server of the FW beforehand. Only these authenticated users can remotely log on to the Firewall. After successful logon, users can access several modules of the FW for configuration, management and monitoring purposes. Smartview Monitor is the module of monitoring and report generation and it has a list of predefined reports. In addition, Smartview Monitor module presents users more capabilities to produce their own reports.

The list of the predefined reports is transferred to the SMS web page of the internal FW. Besides the list, some of the important graphical, real-time reports are displayed on the web page as well. The web page is designed to switch the graphics as the user selects from the list but most significant of the graphics are set to be default ones. One default graphic on the web page of the SMS Internal FW is about the real-time traffic flow of the network with the types of the traffic on the application layer. The other default graphic monitors the names and the source IP addresses of the users who pass through the firewall and reach out the DMZ and Internet.

Anybody who monitors the web page of the FW on a regular basis, can build up a profile of the firewall. This profile is about the routine, regular or repeated performance activities such as the changes of the traffic load during the daytime ,or the most active users during the different periods of the day and the most visited destination. When the network activities are alike on daily basis, similar reports and graphs are generated everyday. Once something unfamiliar or abnormal happens, the indicators of the FW change and an unusual graphic or table is produced. This situation is detected by the network devices and an alarm may also be produced to warn the administrators. However, users who are regularly monitoring the SMS can easily detect this difference and deviations independent of the alarm messages.

#### **4.4.4. External Firewall**

The external firewall is the first frontier of any organization's network against attacks coming from the Internet; therefore it is located between the company network and the outside world. This firewall's role is very crucial since it acts as the gate that opens to the world and acts as the bridge that connects the users to the Internet. If the performance of the firewall fades, all the organization's connection to the outside world is affected. External Firewall faces the first waves of network attacks and withstands those attacks. These attacks may in the form of an excessive number of packets such as distributed denial-of-service (DDOS) attacks, and the firewall may be in a position to handle extreme amounts of network traffic. Thus its performance parameters should be monitored regularly. It should be kept in mind that any network attack changes the routine performance profile of the firewall instantaneously.

In the model network, Juniper's Netscreen 500 is used as the external firewall. The firewall is a hardware-software combination. It has its own software running on

its own hardware. There are three different ways of managing, monitoring and configuring the firewall: a web-based interface, a remote management tool (Netscreen Security Manager – NSM) and a command line tool. The web-based tool is effective for configuration purposes and hardware performance monitoring, while NSM is good for both configuration and FW monitoring. The command line tool is an emergency backup. In this study, the web based tool and NSM are used together to manage the firewall.

The web page of the firewall presents critical performance parameters about the Netscreen firewall as tables and graphics. One of them is the device information table, which displays the hardware and firmware version number of the device. There is a resources status graphic, which exhibits the CPU and memory utilization rates with the number of the sessions and the number of the policies applied on the device. Other graphics include the most recent alarms and events related to the firewall activities and logged on users. One other table shows the network zones that the interfaces are connected and their statuses. Since the device is a firewall, the statuses of the interfaces are very critical performance indicators. The SMS web page of the external firewall is presented in Figure 4.5.



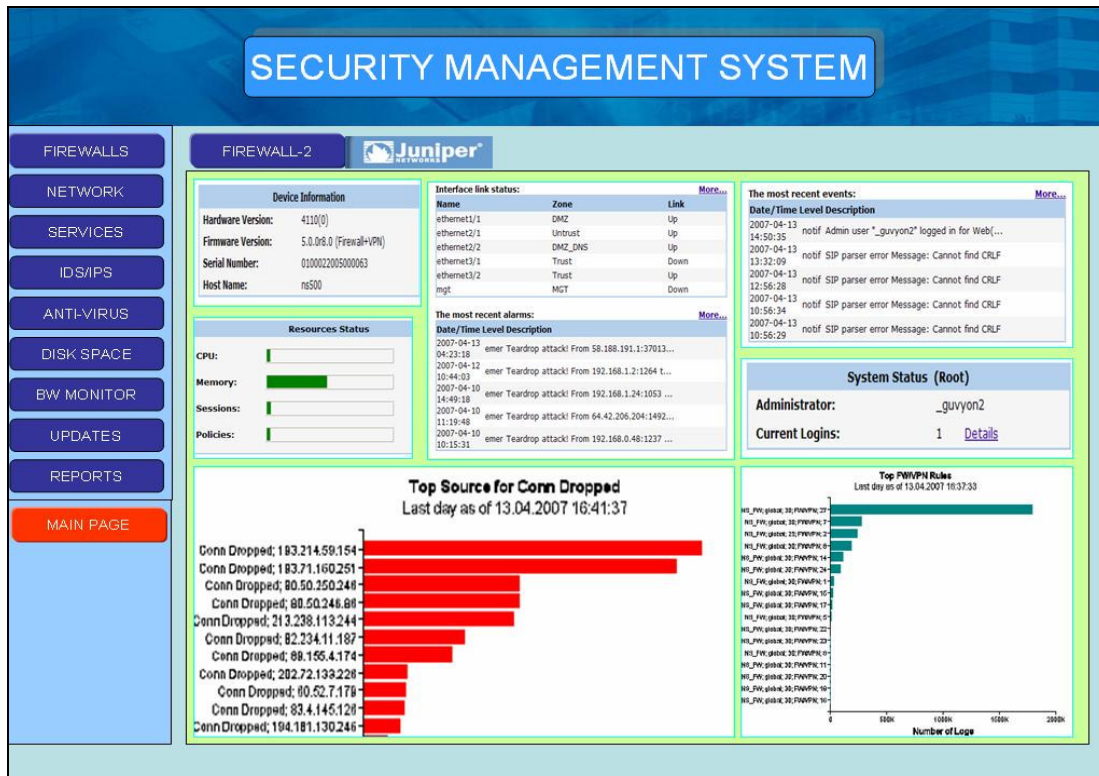


Figure 4.5 Web page of the External Firewall

On the lower part of the web page, the reports related to the network activities and traffic analyses are presented. On the model network's external firewall SMS web page, two reports are displayed. One of the reports is about the sources for the refused traffic and the other is about the most frequently used firewall rules. The reason for monitoring these reports is similar to the profiling explained in the internal firewall section: to monitor the daily traffic routine of the firewall and prevent any possible attacks in advance.

The reports presented in the lower part of the web page are taken from the NSM module. Similar to other network security devices, the important point is to build a profile about the network traffic. By checking out the periodic reports on this

page, a user can easily detect an anomaly. As an external firewall, the most important network traffic parameters are the types of the network traffic, the sources and the destination of the network traffic coming to the organization's network. Since many organizations run a web page and an e-mail service, there should always be traffic coming into these servers. This traffic load makes these servers the most vulnerable organizational assets. Any harm to these servers will not only prevent access to the web and e-mail services, but also deteriorate the organization's reputation.

#### **4.4.5. Intrusion Detection System (IDS)**

Intrusion Detection Systems (IDS) are passive security devices, which analyze the network traffic, find out the suspected traffic and present these findings to the administrators. In order to route all the network traffic to the sensors of the IDS, on one of the bottleneck switches of the network, all the traffic should be mirrored to one port of the switch and this accumulated traffic should be routed to the IDS sensor. IDS sensors analyze the traffic and send out their findings to the management console. In addition to these detection capabilities, in some IDS systems, there are prevention capabilities as well. This capability is used to block some predetermined malicious traffic.

In the sample network, ISS's Realscure Siteprotector is used as IDS. This IDS has a sensor and it is located in between the two firewalls as the Control Manager server. The IDS management server is a Windows 2003 server in which the logs and the reports are produced and saved. The traffic that passes through the external firewall in both directions is analyzed by the IDS. Realscure Siteprotector uses signature based detection effectively. ISS Realscure has the largest amount of attack signatures compared to its rivals. ISS maintains a team of experts called X-force. This team is responsible for finding out vulnerabilities and writing down

possible attack signatures about these vulnerabilities. Attack signatures are labeled with either one of the importance levels: high, medium and low. In real time, the ISS management console presents the number of attack signatures that the system catches. Besides the signature detection technique, Siteprotector is also capable of detecting the attacks based on the traffic and system abnormalities. The web page of the IDS is presented in figure 4.6.

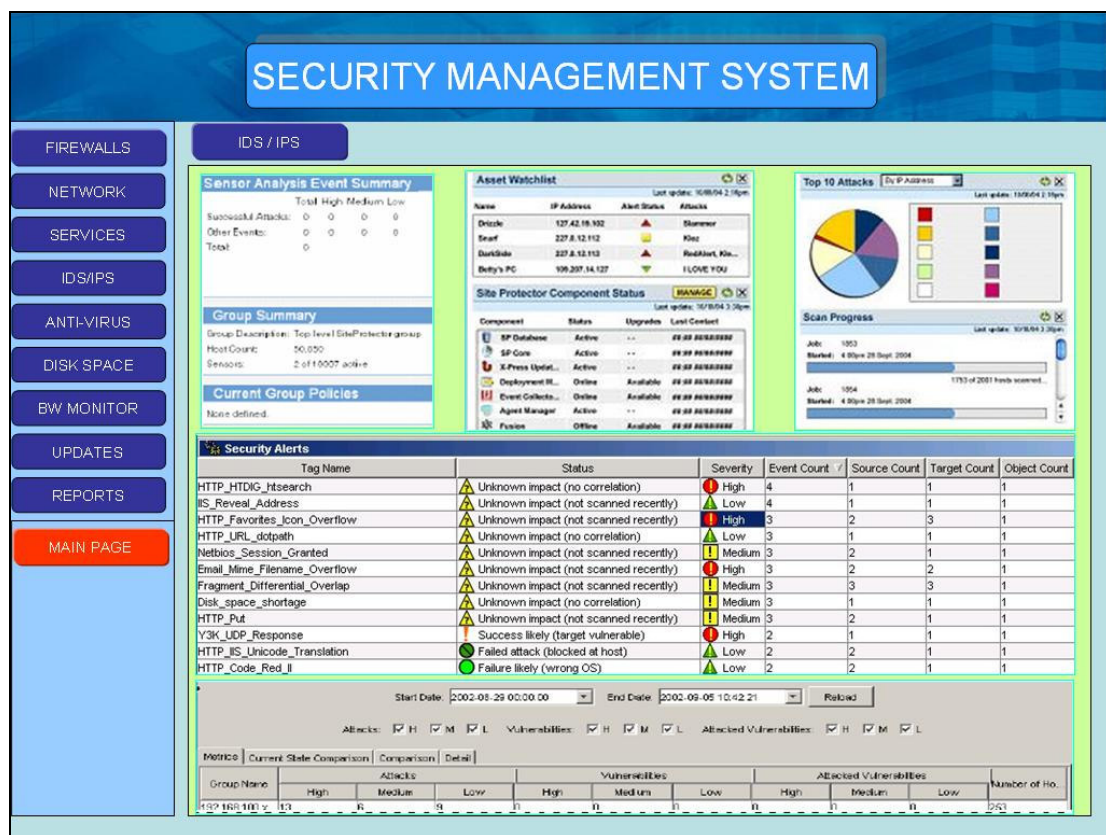


Figure 4.6 Web page of the IDS

On the main page of the SMS, the number of the attack signatures is presented in order to give a general idea about the number of the activities at a given time during the day. On this IDS web page of the SMS, presented in Figure 4.6, detailed information is available. On the web page, there are tables about the number of

events, the statuses of the components of IDS, and a graphical presentation of the top 10 attacks of the day. On the lower part of the page, in the “security alerts” table, the events are presented to the user on a real time basis. This table is taken from the central management console of the Siteprotector. Siteprotector has an interactive interface where the users can make successive queries to find out the reasons of attack logs. When users right-click on an event in the security alerts table, a list is displayed. The list has a number of options about that event, such as the destination of the attack, source of the attack and the explanation of the attack. Choosing one of the options changes the content of the page accordingly. Since the table in the SMS web page is taken from the Siteprotector, it has the same capabilities of right clicking and changing the contents of the table. The last part of the page shows the search screen. By the help of this screen users can look for a specific event which happened on a specific date. The results of the queries are displayed via a pop-up screen.

#### **4.4.6. Anti-Virus System**

Anti-virus software is as an active defense system. There are two different versions of the software being used on the organization’s sample network. One of them is used for e-mail protection while the other one is used for web traffic protection. E-mail protection software is installed on a server and that server is configured to check the incoming e-mails before it reaches the organization’s e-mail server and outgoing e-mail messages before they are delivered to their destination e-mail servers. There are also other modules of the software that can be installed on the e-mail server to scan the e-mails, which are delivered inside the organization’s network. Web traffic analysis software is installed on a server, on which the web traffic passes through. This server analyzes the traffic and prevents suspicious traffic.

In the sample network, Aladdin's E-safe software is used for both purposes. E-safe is managed through a user tool called E-console. This tool is installed on the administrator's computer and after running it; it connects to the servers on the network. By the help of the tool, servers are configured and the logs are monitored and analyzed. The main page of the SMS presents a table, which contains the basic information about the activities of the two anti-virus software: names, amount of the load, numbers of the blocked, queued or allowed packets and the CPU consumption rates.

One of the most important parameters that should be checked on any Anti-virus software is the date of the last update. Since the time gap between the vulnerabilities and the exploits are getting smaller everyday, the importance of the updates is becoming extremely important. An out-of-date anti-virus software has little, if no chance to be effective against the new viruses. The table on the main page of the SMS also presents the latest update time of the software to help the administrators make sure that their system is up to date.

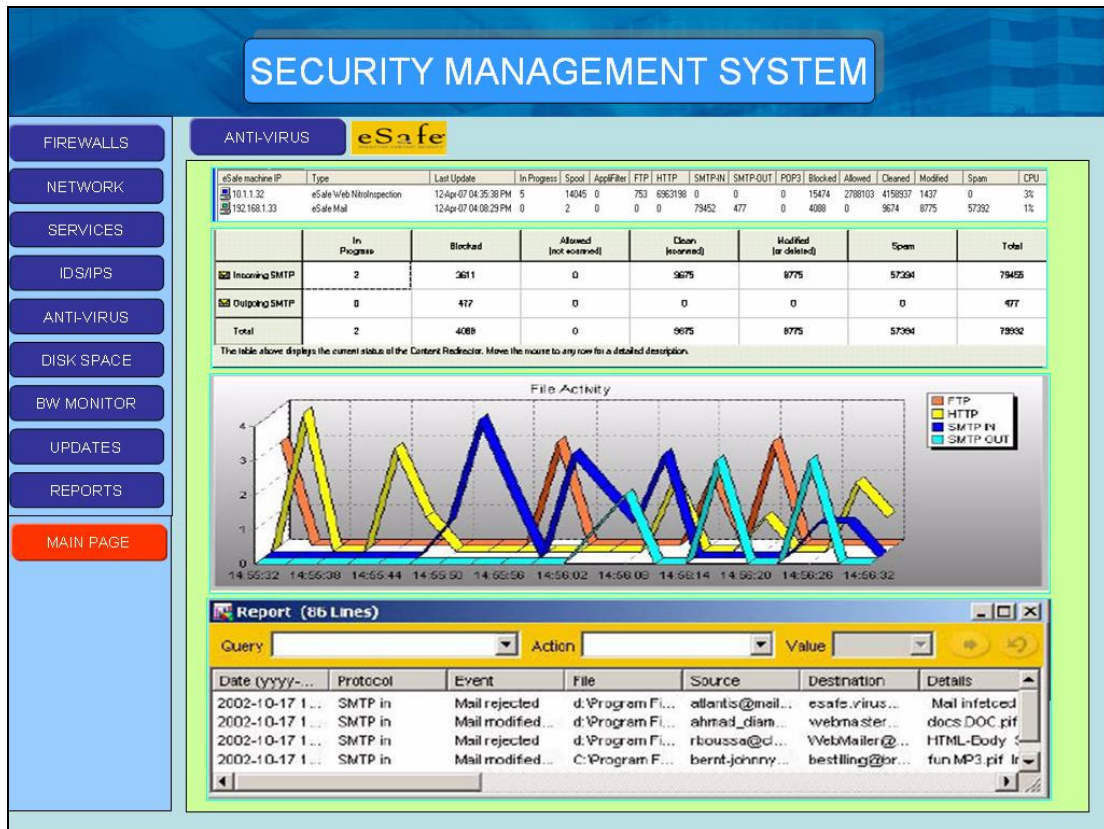


Figure 4.7 Web page of the Anti-Virus Software

The web page of the anti-virus software is shown in Figure 4.7. Additional information and graphics are presented on this page. The graphics are about file activities on the servers, which are monitored by the anti-virus software. There is also a detailed table about e-mail activities according to their origin and destination. The last part of the page has a search screen through which the administrator can make queries such as the destination and source addresses of the spam and infected e-mails. These queries are helpful for finding out the malicious sources and taking the necessary precautions against them. Another benefit of the query screen is its redirection capability. Anti virus programs have a margin of false-positives. False-positives are the regular traffic, which is blocked by the detection algorithms of the software. For most popular anti virus products, false-positive rates are below 1%. If one e-mail, despite being a normal one, is blocked by the anti virus program, it can be

sent to the recipient by the administrator. This task is fairly easy and can be carried out on the SMS web page of the IDS, presented in Figure 4.7.

#### **4.4.7. Network Monitoring**

Network monitoring is important for the availability of the servers and other critical network devices. The software used on the sample network is Computer Associates' SLM. The software is configured to send out ping packets on a continuous basis. The software receives the ping response packets and according to the number of the responses, it calculates and presents the availability of the network on a percentage rate. This data is presented on the main page of the SMS. On the corresponding SMS page of the network monitoring, more detailed information is presented. The SMS page of network monitoring is shown in Figure 4.8.

The SMS page of the network monitoring is taken from the web page of the SLM software. It gives the opportunity to the administrators to look for the availability statuses of the devices for a predetermined period. After selecting the date, an administrator can see the availability statuses of the servers and the times they were up and down. The availability rates of all the servers are presented in the same row. In the model network, the software is configured to display the results for the last week.



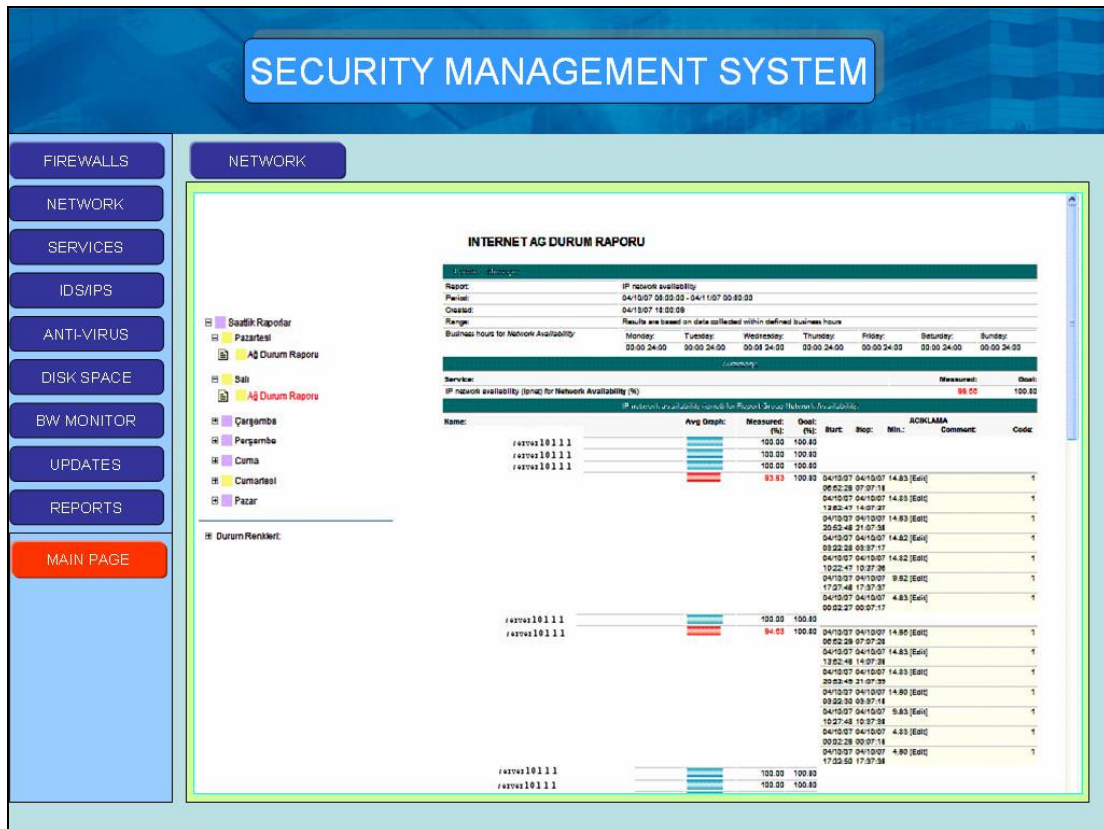


Figure 4.8 Web page of the Network Monitoring Software

#### 4.4.8. Bandwidth Monitoring

Every organization has a network infrastructure built on a network technology such as ATM, Gigabit Ethernet and Frame Relay. These network technologies have an upper limit of bandwidth availability, which is generally either 10 Mbits/sec or 100 Mbits/sec or 1 Gbits/sec. The capacity of the network technology corresponds to the internal bandwidth capacity of the organization. Besides the internal bandwidth capacity, organizations have a more limited bandwidth capacity when they connect to the Internet. Internet connection capacity is determined according to the organizations needs. Besides, organizations should pay a fee to an Internet Service Provider (ISP), which increases with the capacity of the connection. Thus, the capacity must fulfill the needs of the organization and be affordable as well. High rates of bandwidth



consumption may be a problem area in which there will be no connectivity and availability problems but the network may still suffer. The source of the problem may be excessive amount of Internet usage by the employees or may be a Denial-Of-Service type of attack.

Monitoring the bandwidth consumption can help taking preemptive precautions against attacks and may help spend the company resources more effectively. The bandwidth management software presents the real-time and historical graphics to the users. The main page of the SMS has a graphic about the amount of the real-time IN traffic. On the web page of the Bandwidth Monitoring tool, there are graphics for both IN and OUT traffic. There are also links for historic graphics such as monthly and yearly ones. Besides the graphical presentation of the bandwidth consumption, there is also a capability of defining alerts on the software. The alerts are also presented to the administrators as one of the tabs of the BW Monitoring software on the web page of the SMS. The BW monitoring web page of SMS is given in Figure 4.9.

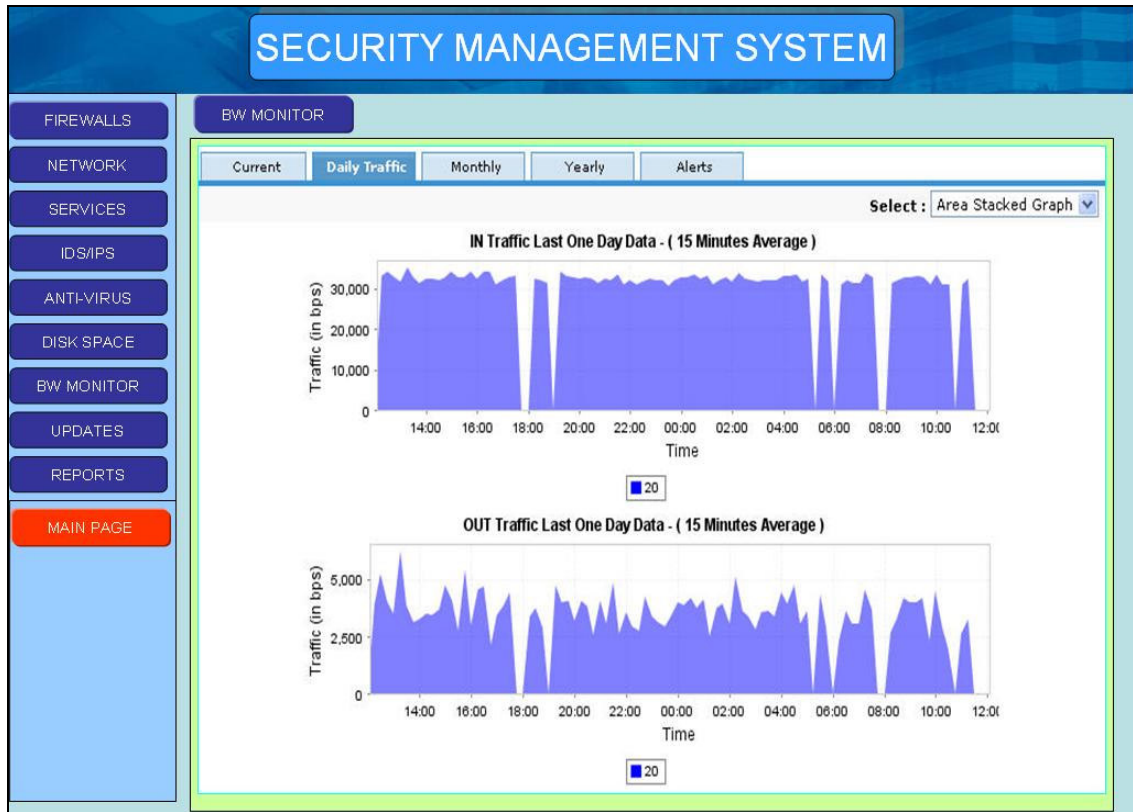


Figure 4.9 Web page of the Bandwidth Monitoring Software

#### 4.4.9. Disk Space Monitoring

Disk space is another important parameter for the servers, which should be up, and running all the time. Once there is no more free space on the disk of a server, that server cannot function properly and becomes unavailable. The goal of monitoring the disks is to prevent any unwanted interruption of the services on the critical servers. After installing the software on a privileged server, the servers that will be monitored should be defined on the software with their related disks. After proper configuration of the software, the disk space monitoring software checks the capacity usage of the disks on a continuous basis. The results of these checks are presented on the web-based interface of the program.

There is a small box for the results of the disk space monitoring software on the main page of the SMS. In the box, the number of the disk errors is presented. In order to view the details of the errors, users must click on the box and reach the SMS web page of the disk monitoring software. On the web page of the disk space monitoring software, the disks of the servers that are over the predetermined levels are labeled with red. This change of color is an indicator for administrators about the disk space related problems. The SMS web page of the disk space monitoring software is presented in Figure 4.10.

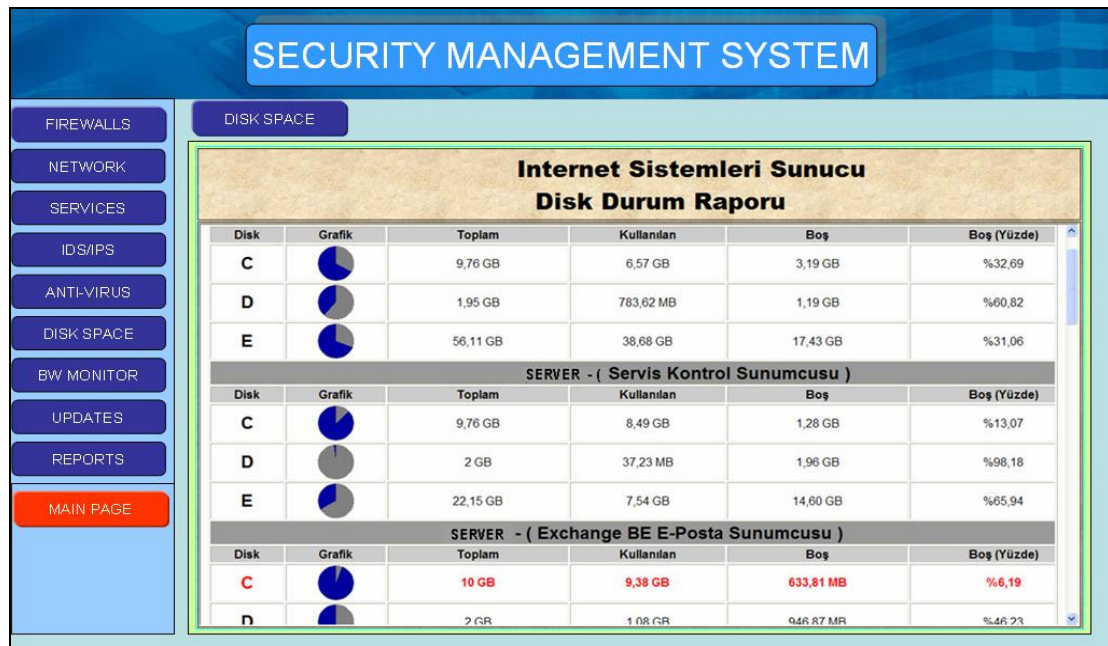


Figure 4.10 Web page of the Disk Space Monitoring Software

After reaching the main page of the Disk Monitoring Software, users can see the disk space usage rates, which are presented in a table with a pie chart. The table gives information about the full capacity of the disk, used space, free space and the percentage of the free space on the disk. If the used space on the disk exceeds the predetermined percentage, an error message is produced and the fonts of the information in the row become red.

Disk space monitoring is not a dedicated task of security administrators; however it is the responsibility of all the administrators. The consequences of the errors in disk spaces are widespread and administrators who are responsible of running servers in the organization's network are prone to these negative consequences.

#### **4.4.10. Service Status Monitoring**

Many important programs run as a service on Microsoft Windows servers. Quite a few windows components and software products such as IIS and Microsoft Exchange service also run as a Windows service on the servers. These services should always be started when the server starts and should not be stopped at anytime. Besides the services that should be running all the time, there are also several windows services, which should be deactivated according to the level of security hardening applied on the server. Managing the services on the servers is a critical task. The stoppage of a necessary service can make the server obsolete while an unnecessary service running on the server may give the opportunity to the hackers to gain access to vital corporate data.

Service status monitoring software is designed as a Windows script which checks the status of the predefined services on the servers periodically. The results of the checks are presented to the administrators via a web page (Figure 4.11). In order for the software to run properly, every critical service on the servers should be defined on the software and the changes should be applied immediately.

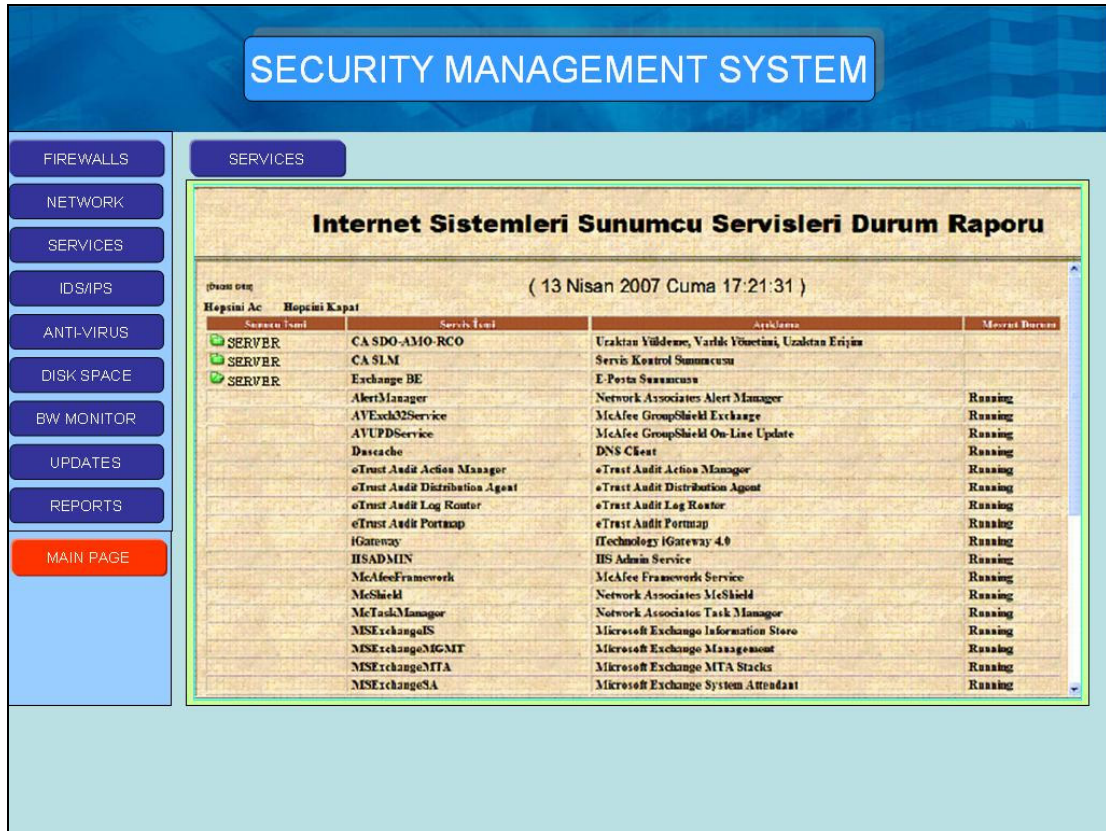


Figure 4.11 Web page of the Service Status Monitoring Software

Similar to the disk space monitoring software, the service status monitoring software also has a small box on the main page of the SMS. In this box, the number of faulty services is presented to the administrators. After seeing the warning message on the main page, administrators, by clicking on the box or on the tab in first section, reach the service status monitoring web page of the SMS.

On this web page, a table is presented to the users. The names, critical services of the servers and short explanations about services are given in the table. The final column of the table indicates the current status of the service. If the status of the services is different than the default value, the fonts of the information in that row change to red and an explanation note is presented on the rightmost column.

#### **4.4.11. Update Status Monitoring**

Many organizations prefer Microsoft Windows operating systems for their client and server computers. When the operating system is chosen as Windows, server software is also selected from the Microsoft product family. Microsoft Office, Exchange and IIS are among the most common popular software of the Microsoft product family.

The burden of Microsoft products is the security vulnerabilities. In order to fix the security related problems, software companies should provide the patch of the problem. Microsoft, being the leader of the software industry in the world and also the leader of patch providers, continuously improves its patching systems. The latest patching software is Windows Systems Update Service (WSUS). By the help of WSUS, administrators can easily manage the patches in their network. The system works in a fairly simple manner. When WSUS is installed on a privileged server, it scans the network range and creates the patch inventory of the organization. Later on, it connects to the Windows updates web page and downloads the list of the available patches. It makes a cross check between the list and the patches on the computers. At the end of this check, WSUS presents the findings and waits for the input of the administrator. The administrator selects the appropriate updates and WSUS applies the patches accordingly.

WSUS is managed and monitored via a web interface. The interface has a main page and several related report pages. The most important part of the main page of WSUS is the summary section. This section is displayed in the main page of the SMS. In this part, the summary of the WSUS and the network is displayed. This summary includes the total number of computers in the network, total number of approved and denied updates, total number of faulty patch installations, and total

number of computers which need at least one update. By clicking on this box or by selecting the tab on the first section, users can access the web page of the WSUS on the SMS. The web page of the update status monitoring software is presented in Figure 4.12.

At the very top of the page, a graphical presentation is given which reflects the overall information about the computers in the inventory. In the middle part of the web page a list of things-to-do is given. This list is helpful to the administrators while planning their work hours. The last part of the web page contains the reports of the WSUS software. The user can select any parameter and make queries about the patches' and the computers' status.

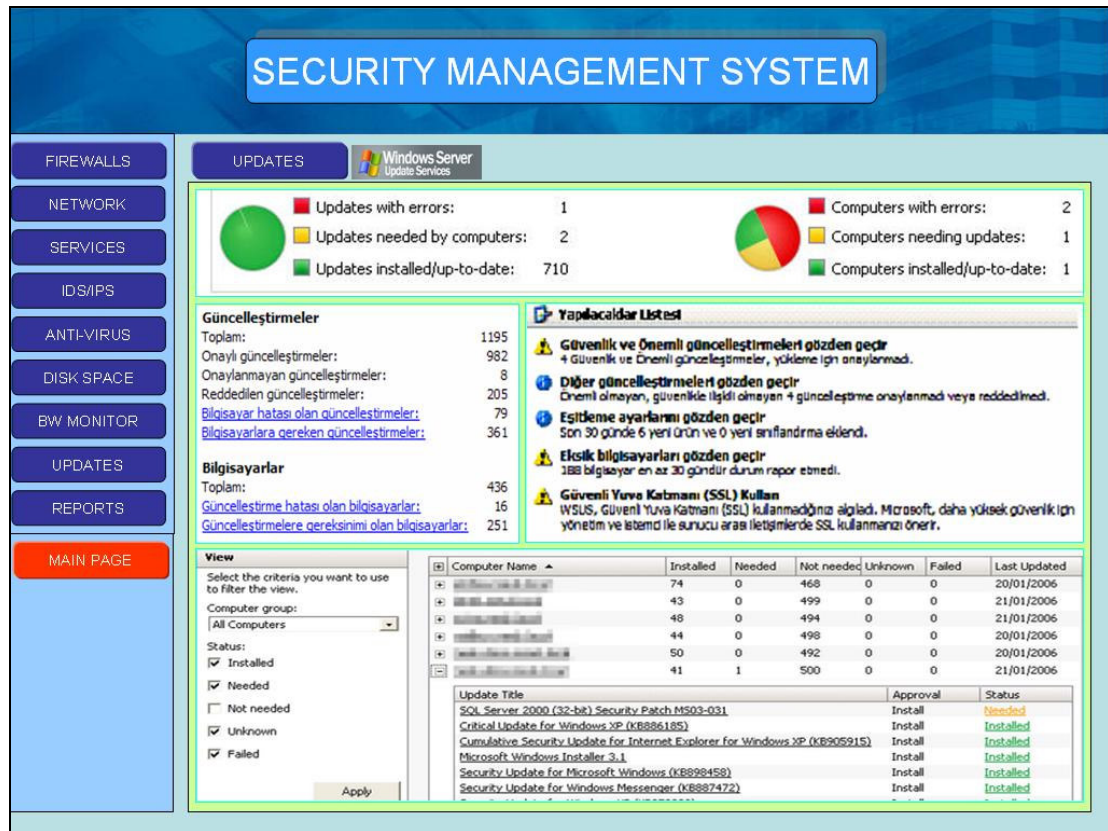


Figure 4.12 Web page of the Update Status Monitoring Software



#### 4.4.12. Reports

The final page of the SMS is dedicated to the reports. Even though the main goal of the SMS is making reporting easier, it does not eliminate the need for standard reports of the security devices. Routine reports of the devices are kept in the SMS server and presented to the user via this reports web page. The reports page of the SMS is presented in Figure 4.13.

There are two main sections in the reports web page: one is for the recent reports and the other is for the old reports. The recent reports section presents the reports that are generated in the last month. Once the report becomes older than a month, it is transferred to the reports repository section. The report repository section contains the past reports and saves them for one year for future use such as a forensic search. The section has links for all the devices. The links, when clicked on, open a pop up window and present the past reports.

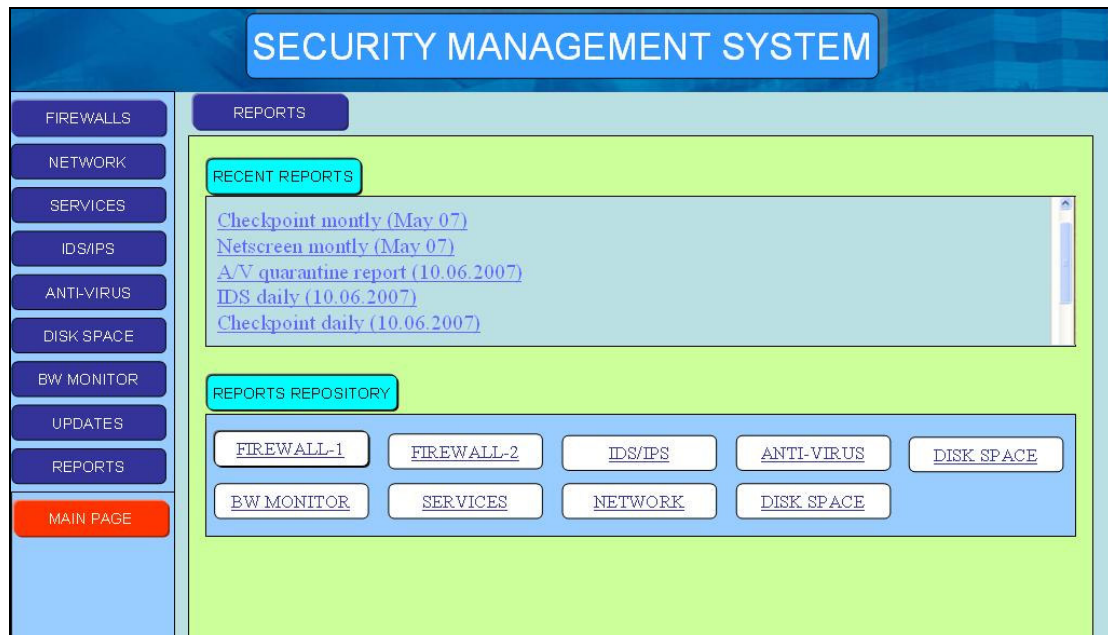


Figure 4.13 Web page of the Reports



## **4.5. Conclusion**

Based on the problem areas mentioned in previous chapters, an SMS solution is proposed and described in this chapter. This solution provides a flexible web application that can be tailored for any network scheme. The main feature of the SMS application devised for the model network and the details of the SMS web pages are presented, emphasizing the major security management issues that have been covered. For the network model presented in this study, some of the tools of SMS have actually been activated and tested. Network monitoring, disk space monitoring, and service status monitoring are the three tools, which are operational in the SMS.

For the network monitoring tool, Computer Associate's Service Level Management (SLM) tool is used. This tool presents the results over the web. The web page of the SLM is modified to cover the servers in the model network. Disk space monitoring and service status monitoring tools are custom made for the model network using HTML coding and Microsoft scripting language. The codes of these tools are written to cover the needs of the model network and they may differ for other applications.

## **CHAPTER 5**

### **DISCUSSION AND CONCLUSION**

#### **5.1. Discussion**

The web based security management system (SMS) presented in this thesis, overcomes most of the shortcomings of the old decentralized way of managing the security of a network. The proposed model provides web-based interfaces, which display the performance indicators of all the security devices in the organization's network.

With its useful features and advantages, SMS helps security administrators to handle their task conveniently, and provides a better way of presenting the security issues to upper management. The advantages of SMS are better convenience, reduced time for monitoring, centralized presentation of the logs, user-friendly interface, better way of troubleshooting, modular and scalable design, and centralized storage of the reports. These advantages are explained in detail in the following sections.

After the implementation of the SMS, network management became significantly easier. Administrators who are on duty after work hours monitor the performance of the system in a more convenient way. The thresholds are determined through the system and based on those parameters, the on duty personnel are given specific instructions to act. These precautions prevent false alarms that had to be dealt with. SMS also made network monitoring easier during the work hours. The upper management and administrators can see the real-time status of the network, the status of the services and the disk spaces when they check the web pages of the system.

### **5.1.1. Better Convenience**

In the proposed template, the computers in the organization's network are connected to one another by a local area network. This connection is a solution to many of the paper-based applications in the organizations. With the help of SMS, paper-based report generation is no longer needed. The reports of the devices are added to the 'reports' web page of the SMS. The reports can be downloaded by anyone with permission to access the web page. The upper management of the organization can use this page to download and examine the reports.

Besides the routine reports, upper management can also monitor the security position of the organization anytime during the day. Since SMS provides a centralized and user-friendly interface, it becomes easier for anybody to monitor the performances of the devices, regardless of their background and knowledge in computers and security.

The SMS enables security administrators as well as top management to monitor the overall security of the organization in real time. The main performance parameters of all the selected security devices are placed on a single web page. The page is updated as the parameters change and any abnormal activity can be detected as it occurs.

Through the use of SMS, administrators are only responsible for monitoring the main page of the SMS. They may examine the other web pages if any kind of abnormal behavior is indicated on the main page. Reaching the specific web pages of the devices is simple with SMS. All the devices are just one click away. All the web pages of the devices present adequate and summarized information about the

performance of the device. Besides the summarized information, there are times when specific information is needed for an investigation. If any additional information, like the access records of an internal user or the network activity of an external source is needed, administrators can still use the interface of the device and troubleshoot the problem.

### **5.1.2. Reduced Time for Monitoring**

The new system reduces the time spent by administrators when logging into several devices and checking out the logs of those devices separately. Before, the administrators had to install the user consoles of all the security devices and monitor their pages in those separate windows. On the other hand, SMS is a single web page that combines all the information presented by the respective tools of the devices. Without the use of a centralized management interface such as SMS, the screen of the administrator is cluttered with several web pages and interfaces of the devices which is not a convenient way of handling security. By the use of SMS, administrators can save time, and focus on their job more efficiently.

One of the most important precautions against network attacks is being alert all the time and prevent the attack as soon as possible. The best way of being alert is real-time monitoring of the indicators, which can signal the attack as it happens. The SMS system provides the means necessary for early reaction. As SMS is monitored carefully, clues about a network attack can be detected instantaneously.

### **5.1.3. Centralized Presentation of the Logs**

Usually, the logs of the each security device are stored on their own servers and can be viewed by only the help of their own interfaces. This situation causes difficulties for administrators when dealing with more than one device simultaneously. By the help of SMS, the logs of different devices are presented in one centralized web page. SMS contains a web page for each security device and if needed, the log query pages of the security devices can be added to the web page. As the result of such a configuration, administrators can search for incidents in an easier and timesaving manner.

### **5.1.4. User-friendly Interface and Ease of Navigation**

Besides providing means for better monitoring and management, the proposed model has better presentation capabilities. One of the features of SMS is its attractiveness for the user, because of its user interface. It presents routine reports and real-time performance indicators of the security devices via user-friendly interfaces, which is a convenient way of informing upper management about the security-related activities.

The main page of SMS presents the most important information to the users. If the user moves the mouse over the graphs, the icon of the mouse changes and indicates the clickable places on the screen. When the user clicks anywhere on the graph of a security device, the SMS web page of that security device appears. For reaching other pages, there are tabs with the names of the devices on them in the first section of every page. After reaching and examining a page, there is a red tab on the first section of every page for going back to the main page. The report page of SMS has the list of available repots. Once the user clicks on a report, the report in PDF

format is opened in a pop-up window, which lets the user visit the other pages independent from the open report. As the result of these features, there is little chance of losing track when surfing the web pages of SMS.

#### **5.1.5. Better Way of Troubleshooting**

Troubleshooting requires cross checking an alarm, which is taken from one security device such as an IDS. In order to verify the validity of an attack, the administrator should check other security devices to find the evidence of the attack. Finding out the source, destination and the type of an attack is the starting point of countermeasures. SMS provides the environment for the security administrator to make checks for any of the alarms or abnormalities. The design of the web pages allow users to complete a cross check over the security devices in a very short time.

#### **5.1.6. Modular and Scalable Design**

The new system is suitable and scalable for any organization regardless of its size and the variety of security devices it has. In order to adopt SMS to a network, devices can easily be added to SMS, and web pages for those devices can be created in a very short time.

#### **5.1.7. Centralized Storage of Reports**

The routine reports of the devices are stored in a central server, where administrators and upper management can easily find what they need. By providing a central storage for reports, the handling, storing and presentation of the reports become independent of the administrators. Reports are added to the web page and

anybody looking for a specific report can go to the web page and download the report.

## **5.2. Conclusion**

The new web based security monitoring system, SMS, possesses the necessary capabilities that an administrator needs when performing security related tasks. Moreover, the system is modular, flexible, scalable, and user-friendly. These features make SMS a convenient solution for security management.

The implementation process of SMS is simple since web page design is facilitated by tools like Microsoft FrontPage and Macromedia Dreamviewer. In web page design, it is easy to reuse a piece of code by copying it from a web page and transferring it to another one. Thus, new pages can be created by reusing the code from the web pages of existing devices. These devices are the problem-free modules of SMS. In addition, the programs custom designed specifically for the organization, like the disk space monitoring software, can be implemented as easily as the problem free modules.

For devices that have their own management and monitoring consoles and tools, the coding of the web pages requires additional knowledge along with web page design capabilities. Besides, some legal and license problems may arise since these software are copyrighted and not permitted to be used by third parties for other purposes. If their vendors are not willing to open their source codes to the organization's programmers, it becomes more difficult to construct and integrate the web pages of these devices into the SMS.

For the network model presented in this study, some of the tools of SMS have actually been activated and tested. Network monitoring, disk space monitoring, and service status monitoring are the three tools, which are operational in the SMS. Netscreen 500 firewall, Nokia IP server and WSUS have web interfaces, and thus they constitute the problem-free modules of SMS. These modules are not integrated into the SMS yet, however their pages can easily be designed and integrated into SMS. However, Checkpoint FW, E-safe Anti-Virus Software and RealSecure Siteprotector IDS are not as easy to integrate as the other modules, since they use their own software for configuration and monitoring purposes. The integration of these three modules depends on the consent of their vendors for using their source code, and the cooperation of their technical staff in reusing the code in SMS. If the vendors agree upon on these two topics, the modules can be created and added to the SMS. If the vendors refuse to cooperate, those modules of SMS can not be completed as proposed.

Table 5.1 compares SMS with TriGeo's Security Information Management (SIM) software, which is one of the most popular commercial central management products. SIM was chosen by SC magazine as the best Security Management Software (Stephenson, 2006). The comparison parameters in the table are evaluated by the author and graded according to the functionality of both tools. Based on the results of the comparison, it is clear that the strength of the system developed in this study (SMS) provides a cost-effective alternative to commercial central management software (SIM). Even tough, correlation and aggregation capabilities of commercial products are superior, the ease of use and cost-effective features of SMS makes it appealing to organizations. In addition, the proposed model, when implemented fully, provides many of the capabilities of its commercial equivalents.



Table 5.1. Comparison of SMS with TriGeo's SIM.

<b>No.</b>	<b>Criteria</b>	<b>Security Management System (SMS)</b>	<b>TriGeo's SIM</b>
<b>1</b>	Ease of Use	Excellent	Good
<b>2</b>	Rule Base, Artificial Intelligence Application	Poor	Good
<b>3</b>	Set up, Configuration and Implementation	Good	Excellent
<b>4</b>	Custom Reports	Poor	Good
<b>5</b>	Price	Excellent	Average
<b>6</b>	Performance	Good	Good

One of the problem areas that SMS is short of achieving is the correlation and aggregation capabilities, which are helpful for finding out the attack traces among the logs of several security devices. Other commercial alternatives provide different types of artificial intelligence and fuzzy logic applications, which can compare different logs and correlate these logs. These kinds of applications are difficult to program and expensive. Integrating these capabilities require employing experts and allocating funds and time. Since SMS was introduced to provide a cheaper alternative, the integration of these capabilities is beyond the scope of this thesis. However, as mentioned in the thesis, “trigger” is an important issue. The triggers of attacks and dangers are defined in SMS, and SMS can be configured to notify security team members when an incident happens. The administrators can be notified via e-mail, a pop-up alert, or even with a short message or via pager.

During the implementation of SMS, in order to reduce dependence on software vendors, favoring open-source software alternatives is recommended. Open-source alternatives can be integrated to SMS since their code is open to everybody and they do not have licensing and copyright restrictions.

The SMS provides the regular reports of the security devices without any modification. These reports can be modified based on predetermined criteria. Moreover, reports of several devices can be combined in one single report and presented to upper management periodically. The modifications of the reports and combination of several reports in one single report may be another research area for future work.

The flexible design of the SMS allows customizing the software for each network that uses SMS. The installation of SMS requires coding the web pages for that network. If any change in the existing pages of the SMS is needed, the code of the software should be changed accordingly. As a future work area, in order to increase the flexibility to the software, a layer in the software that may ease the addition of a new page or a change in one of the web pages of the SMS can be added. This approach to software coding may make the mass marketing of the tool easier.

## REFERENCES

Abramson, C. (2001). A Return to Legacy Security. *SANS Institute Security Reading Room*, Retrieved April 03, 2007, from [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

Anderson, R.J. (2001). Why Information Security is Hard – An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society, p.358. New Orleans, LA.

Ankara Emniyet Müdürlüğü(2001). Bilgisayar Suçları Sözleşmesi. Retrieved June 01, 2007, from <http://www.ankaraemniyet.gov.tr/?id=601>.

Arconati, N. (2002). One Approach to Enterprise Security Management. *SANS Institute Security Reading Room*, Retrieved April 13, 2007, from [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

Armstrong, I. (2001). Legislators Turn up the Heat on Cybercrime. *SC Magazine April 2001*, 33-34.

Bertagnolio, L. (2001) Security on the Network: What You Need to Know. *SCMagazine, February*.

Cerf, V.G., Leiner, B.M., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G., Wolff, S. (2003). Brief History of the Internet. Retrieved June 15, 2007, from <http://www.isoc.org/internet/history/brief.shtml>.

Cisco Systems. (2002). Evolution of Firewall Industry. *Cisco Systems White Papers*, Retrieved January 22, 2007, from [www.cisco.com](http://www.cisco.com).

Cisco Systems. (2006). Network Security Policy: Best Practices White Paper. *Cisco Systems White Papers*, Retrieved February 10, 2007, from [www.cisco.com](http://www.cisco.com).

Cohen F. (1987). Computer Viruses: Theory and Experiments. *Computers and Security*, 6, 22-35.

Computer Emergency Response Team (CERT). (2007). Windows Intruder Detection Checklist. Retrieved May 15, 2007, from [http://www.cert.org/tech\\_tips/win\\_intruder\\_detection\\_checklist.html](http://www.cert.org/tech_tips/win_intruder_detection_checklist.html)

Council of Europe (2001). Convention on Cybercrime. Retrieved June 01, 2007, from <http://conventions.coe.int/treaty/en/Treaties/Html/185.htm>.

Hallawell, A. (2004). Gartner Global Security and Privacy Best Practices. *Gartner Analyst Reports*, Retrieved April 02, 2007, from [www.csoonline.com/analyst/report2332.html](http://www.csoonline.com/analyst/report2332.html)

Hyland, P.C., & Sandhu, R. (1998). Management of Network Security Applications. In: Proceedings of the 21st NIST-NCSC National Information Systems Security Conference, Arlington, Virginia.

Ingham K., Forrest S. (2002) A History and Survey of Firewalls. *Technical Reports TR-CS-2002-37*, University of New Mexico Computer Science Department. Retrieved January 12, 2007, from, [http://www.cs.unm.edu/colloq-bin/tech\\_reports.cg](http://www.cs.unm.edu/colloq-bin/tech_reports.cg).

IT Governance Institute. (2006). Information Security Guidance: Guidance for Board of Directors and Executive Management. Retrieved February 15, 2007, from [www.itgi.org](http://www.itgi.org).

Koch, F. (2005), Keeping IT Up to Date, Retrieved 17 May, 2007, from [www.educahelp.ch/dyn/bin/117344-117404-1-ms-wsus.pdf](http://www.educahelp.ch/dyn/bin/117344-117404-1-ms-wsus.pdf)

Kvavik, R.B., Voloudakis, J., Caruso, J.B., Katz, R.N., King P., Pirani, J.A. (2003). Information Technology Security: Governance, Strategy, and Practice in Higher Education. *EDUCAUSE information Technology Security, Vol.5*. Retrieved March 15, 2007, from [www.educause.edu/ecar](http://www.educause.edu/ecar).

Lee, R.D. (2001). Developing Effective Information Systems Security Policies, *SANS Institute Security Reading Room*, Retrieved January 07, 2007, from [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

Martin, M. (2003). Keys to implementing a successful security information management solution. , *SANS Institute Security Reading Room*, Retrieved April 02, 2007, from [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

Michael Espinola Jr's Wiki (2007). Administrator To-Do List. Retrieved April 18, 2007, from [http://www.espinola.net/wiki/Administrator\\_To-Do\\_List](http://www.espinola.net/wiki/Administrator_To-Do_List)

Michael John Muuss, (2007). The Research Interests of MIKE MUUSS. Retrieved April 17, 2007, from <http://ftp.arl.mil/~mike/>

Microsoft Inc. (2007). Ten Immutable Laws of Security Administration. Retrieved March 15, 2007, from <http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.msp?mfr=true>.

Miles, T. (2004). Paradigm Shift. Applied Principles of Defense-in-Depth: A Parents Perspective. *SANS Institute Security Reading Room*, Retrieved April 13, 2007, from [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

Rasmussen, S. (2002). Centralized Network Security Management: Combining Defense in Depth with Manageable Security. *SANS Institute Security Reading Room*, Retrieved April 15, 2007, from [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

Rosamond, G. (2004). Building a more secure network. , *SANS Institute Security Reading Room*, Retrieved April 03, 2007, from [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

Schneir, B. (2005). Managed Security Monitoring: Network Security for the 21st Century. Retrieved March 10, 2007, from <http://www.counterpane.com>.

Setty, H. (2001). System Administrator – Security Best Practices. *SANS Institute Security Reading Room*, Retrieved April 23, 2007, from [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

Stephenson, P. (2006). Group Test SIM/SEM. *SC Magazine, September 2006*, Retrieved 10 June, 2007, from [www.scmagazine.com](http://www.scmagazine.com)

United States General Accounting Office. (1998). *Information Security Management : Learning From Leading Organizations*. Washington, DC Retrieved 10 April, 2007, from [www.gao.gov](http://www.gao.gov).

Wikipedia the Free Encyclopedia. (2007a). History of the Internet. Retrieved 15 April, 2007, from [http://en.wikipedia.org/wiki/Internet\\_history#ARPANET](http://en.wikipedia.org/wiki/Internet_history#ARPANET)

Wikipedia the Free Encyclopedia. (2007b). Computer virus. Retrieved 15 April, 2007, from [http://en.wikipedia.org/wiki/Computer\\_virus#History](http://en.wikipedia.org/wiki/Computer_virus#History)

Willard, M. (2002). Getting the most out of your firewall logs. *SANS Institute Security Reading Room*, Retrieved April 02, 2007, from [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

Zimmermann, H. (1980). OSI Reference Model – The ISO Model of Architecture for Open System Interconnection. *IEEE Transaction on communications*, Vol.Com-28, No.24.