CONSIDERATIONS ON SECURITY MANAGEMENT IN IP COMMUNICATION NETWORKS

Daniel GHEORGHICĂ, Victor CROITORU
University POLITEHNICA of Bucharest, Romania,
gheodan@gmail.com, croitoru@adcomm.pub.ro

Abstract. *The growing popularity of the Internet has taken many organizations by surprise. Established mechanisms such as fax technology, electronic data interchange (EDI), electronic messaging, and file transfers over private networks have dominated electronic commerce until now. However, many of those advantages are shadowed by the lack of widespread use of security and data protection mechanisms.*

This paper is based on the results of research in management and security of IP communications networks, conducted by authors during last few years. Our secure system implementation is able to manage any firewall products that support SSH remote management. We believe that our approach is an important step towards streamlining the process of configuring and managing firewalls, especially in complex, multi-firewall installations.

Keywords: *firewall, security management, GUI, PHP, UML, information security*

I. Introduction

Over the past years, there has been an accelerating growth in the use of network based services. Because of the ubiquity of computer systems and the Internet, this growth will continue. Corresponding to this continued growth in network usage, there will be increases in malicious user activity. The threat of malicious users is becoming more serious every day. Terms such as phishing, pharming, SPAM and identity theft make their way into news headlines all the time. Firewall is a widely deployed mechanism for improving the security of enterprise networks.

Information systems (IS) are exposed to different types of security threats which can result with significant financial loses and damage to the information system resources. The types of damage caused by security threats are different, e.g. database integrity security breaches, physical destruction of entire information systems facility caused by fire, flood, etc. The source of those threats can be unwanted activities of "reliable" employees, hacker's attacks, accidental mistakes in data entry, etc. The financial losses caused by security breaches often cannot be exactly defined because of the facts that significant numbers of smaller scale security incidents are never discovered, a part of incidents are described as accidental mistakes, and all of that is a result of a tendency to minimize the responsibility of a person responsible for the security incident [1]

Information system security threats classifications proposed in [2] addresses the different types and criteria of information system security risks (threats) classification and gives an overview of most common classifications used in literature and in practice. This classification defines a common set of criteria that can be used for information system security threats classification, which will enable the comparison and evaluation of different security threats from different security threats classifications.

We propose a six-level model that identifies the role of security policy, continuity planning, security tools, internal organizational management, and external impacts on the security and integrity of organizational information (Figure 1).

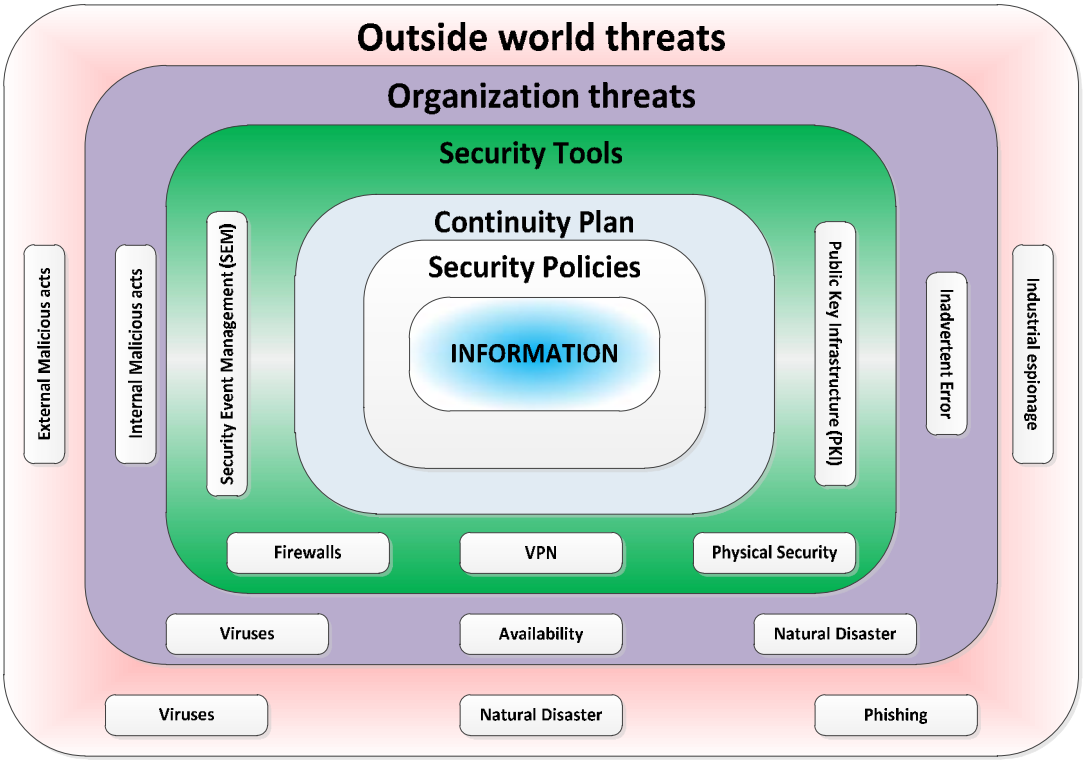

Figure 1. Six-level organizational information security model

A growing security concern is the management of intranets and external networks. With more companies tying their networks into the Internet and allowing more remote access into their systems, security issues are increased. The primary solution to this dilemma has been firewalls. A firewall is a system that has the ability to control the flow of data in and out of a network. Basically, a firewall has two functions: 1) Controlling access and data coming into the network. 2) Controlling data going out of the network. There are two basic approaches to a firewall; either the firewall should permit everything to pass through except what is expressly prohibited, or it should prohibit everything to pass through except what is expressly permitted.

The main component of most firewalls is a screening router. A screening router is a device which has the capability to filter packets of information based on their source and destination IP addresses. Some firewalls are composed of only a screening router using the router as a gateway between the private network and the Internet. However, a simple screening router based firewall does not allow for much flexibility. Therefore it is usually combined with a system to increase flexibility and the ability to control information flow. With the increased functionality, a system can create a firewall configured to control data flow specifically according to an organization's security policy.

This paper proposes a secure system for firewalls management. The system is designed to allow management of all firewalls from a security zone, and is presented in detail in section four off the current paper.

The level of protection that any firewall is able to provide in securing a private network when connected to the public Internet is directly related to the architecture(s) chosen for the firewall by the respective vendor [3].

II. Firewall platforms

Firewall solutions are available on a number of platforms and can generally be segregated into three groups:

- **Hardware-based products** - are single-purpose systems. Required hardware and software are bundled in one easily installed package. Usually, hardware solutions run on a stripped down version of Unix or Linux, where all of the unnecessary Operating System (OS) components are removed. The benefits of this model are that they are fast, relatively inexpensive, and don't require the loading of the software. These solutions require another machine or directory to store and analyze the logs.
- **Software-based products OS** - are software products running on one of the many distributions of Linux or Unix. In some cases, the OS is included in the firewall product, requiring a single install on one low-cost computer.

For some environments, a hardware-based firewall is a great choice. For others, nothing beats a Linux or Unix Software-based firewall.

One of the most misunderstood terms in network security with respect to firewalls today is "OS hardening" or "hardened OS." Many vendors claim that their network security products are provided with a "hardened OS." What you will find in virtually all cases is that the vendor simply turned off or removed unnecessary services and patched the OS for known vulnerabilities. Clearly, this is not a "hardened OS" but really a "patched OS."

A hardened OS is one in which the vendor has modified the kernel source code to provide for a mechanism that clearly provides a security perimeter between the non-secure application software, the secure application software, and the network stack.

III. Firewall policy configuration management

A firewall, like any other network device, has to be managed by someone. Security policy should state who is responsible for managing the firewall, how will be manage and the access method.

Management of firewall policy configurations can be complex, error-prone, costly and inefficient for many large networked organizations. Implementing a firewall configuration policy either involves writing low-level command syntax via a Command Line Interface (CLI) or the use of a graphical management console. Typical errors in a firewall configuration policy range from invalid syntax to errors in properly comprehending the configuration, given its scale and complexity. The Graphical User Interface (GUI) is the most commonly used method to configure a firewall in a timely manner, especially amongst inexperienced administrators.

Actual firewall configuration tools allow individual management of the security policy. When the management of different firewall policies is required it must established one administrative session with each firewall. Each firewall will have its own security policy without any correlation with the policies of firewall from the security area.

Design of the sequence of rules in a firewall must assure that these are consistent, complete, and compact. Consistency means that the rules are ordered correctly, completeness means that every packet satisfies at least one rule in the firewall, and compactness means that the firewall has no redundant rules [4].

Firewalls are the first line of defense visible to an attacker and, by design, are generally difficult to attack directly, causing attackers to often target the administrative accounts on a firewall. The username/password of administrative accounts must be strongly protected, and the administrative channel must also high protected using Secure Socket Layer (SSL) or Virtual Private Network

(VPN) technologies.

IV. Security Management

Like any other network component, a firewall has to be managed by someone. Security policy should state who is responsible for managing the firewall, how will managed it and the access method to the configuration, as a part of security management system.

Management of firewall policy configurations can be complex, error-prone, costly and inefficient for many large networked organizations. Implementing a firewall configuration policy involves either writing low-level command syntax via a Command Line Interface (CLI) or the use of a graphical management console. Typical errors in a firewall configuration policy range from invalid syntax to errors in properly comprehending the configuration, given its scale and complexity. The Graphical User Interface (GUI) is the most commonly used method to configure a firewall in a timely manner, especially amongst inexperienced administrators.

Actual firewall configuration tools allow individual management of the security policy or vendor-dependent multiple firewall configurations. When the management of different firewall policies is required it must be established one administrative session with each firewall. Each firewall will have its own security policy without any correlation with the policies of firewall from the security area [5].

Design of the sequence of rules in a firewall must assure that these are consistent, complete, and compact. Consistency means that the rules are ordered correctly, completeness means that every packet satisfies at least one rule in the firewall, and compactness means that the firewall has no redundant rules [6].

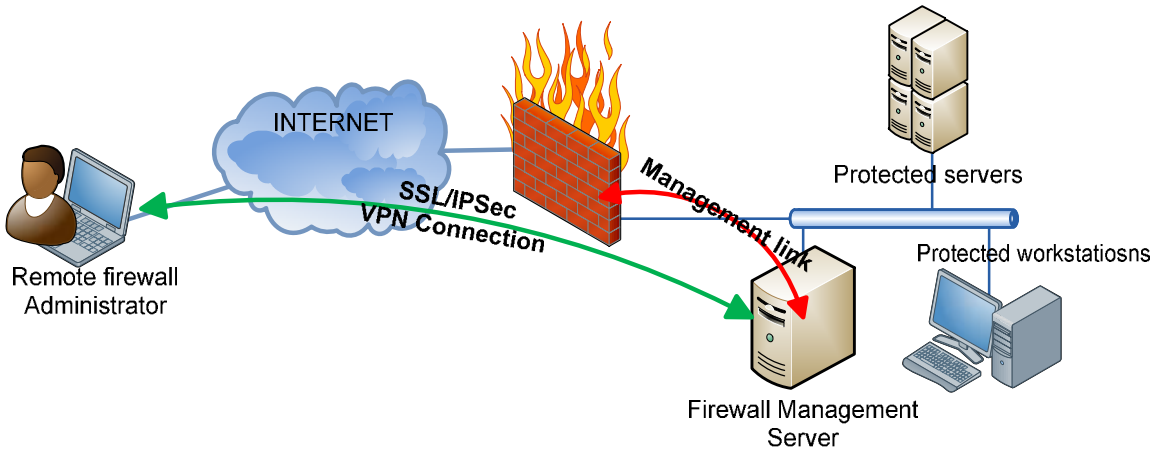

Figure 2. Remote firewall configuration - topology

Firewalls are the first line of defense visible to an attacker and, by design; they are generally difficult to attack directly, causing attackers to often target the administrative accounts on a firewall.

Firewall policy management model provide platform and a framework for developing secure management systems (Figure 2). In [5] is described a system for secured firewall policy management designed using this MVC (Model – View - Controller) model. The proposed model provides a unified top-down view of all network and next-generation firewall policies, from all of the leading vendors. It also supports comparison and analysis of revisions using the vendor's native conventions.

Firewall policy management allows analysis of even the largest, most complex firewall rule bases to identify unused or shadowed rules and objects. Using rules analytic model it can eliminates security loopholes, improves performance, and eases maintenance.

Taking into consideration the high level of security required by information exchanged with

the proposed model of remote firewall management, in the context of security management system, it is necessary to consider a way of assuring this security level. All the communication channels used inside the security management model are encrypted using pre private pre-shared keys or SSL (Secure Sockets Layer) encrypted VPN tunnels (Figure 3).

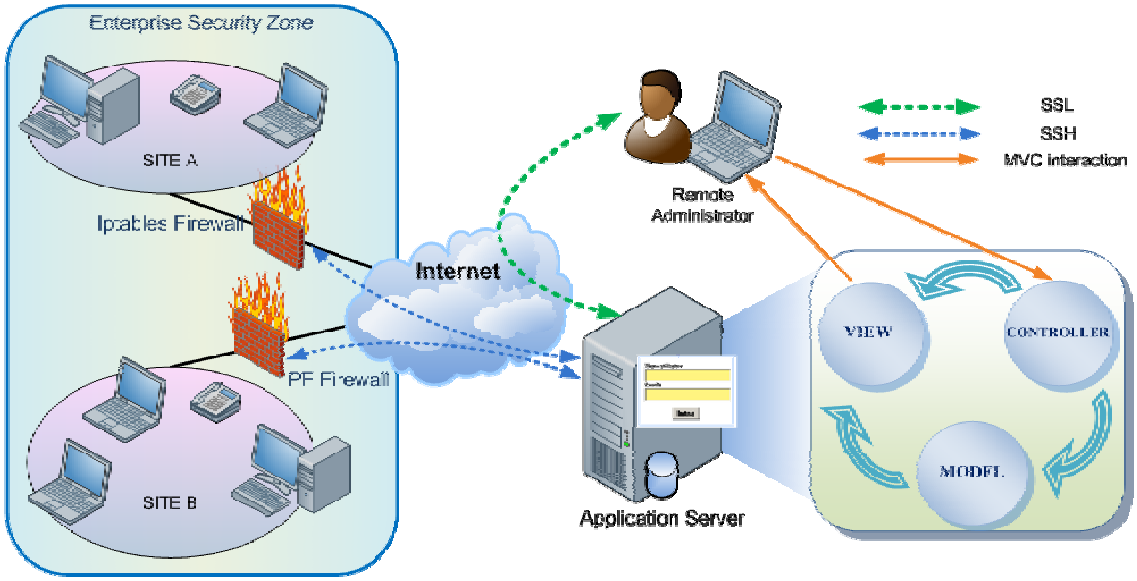

Figure 3. Firewall management within security management system

The system is designed modular in order to allow management of all firewalls from a security zone. Functional and architectural requirements used in the design phase of this system are:

- must be accepted only secure management operations;
- administration of more firewalls from the same interface;
- firewall security policy definition must be rule based;
- firewall rules must be analyzed for security policy compliance;
- full audit on administrative user creation and modification;
- full audit of management operations.

The system has a modular design and is implemented using PHP Hypertext Preprocessor (PHP) based on Model-View-Controller (MVC) model. The MVC model has been developed, from the beginning, in order to model natural "Input - Processing - Output" flow.

The MVC model architecture has its roots in Smalltalk, where it was originally applied to map the traditional input, processing, and output tasks to the graphical user interaction model. However, it is straightforward to map these concepts into the domain of multi-tier enterprise applications.

Components of the proposed system MVC architecture are:

• **Model** - represents data and the activities that govern access to and updates of this data. Often the model serves as a software approximation to a real-world process, so simple real-world modeling techniques apply when the model is defined.

• **View** - renders the contents of a model. It accesses enterprise data through the model and specifies how that data should be presented. It is the view's responsibility to maintain consistency in its presentation when the model changes. This can be achieved by using a push model, where the view registers itself with the model for change notifications, or a pull model, where the view is responsible for calling the model when it needs to retrieve the most current data

• **Controller** - The controller translates interactions with the view into actions to be performed by the model. In a Web application, they appear as GET and POST HTTP requests. The actions performed by the controller include changing the state of the model. Based on the user interactions and the outcome of the model actions, the controller responds by selecting an appropriate view.

V. Conclusions

In the context of rising security requirements and the continuing need for firewall configuration, the proposed security management system appears with his simplicity and usability. The ability to easily manage a firewall configuration is very important in any circumstances. Our proposed secure management system provides a different approach on configuring firewalls. Some of the features of the proposed system are:

- all management operations are secure;
- secure access to management system;
- high scalability and extensibility;
- online firewall configuration backup / restore;
- firewall policy creation, optimization and correlation;
- configuring multiple firewall in the security zone;
- complete operations audit;
- simple and intuitive Web based GUI;
- provides point in time restore facilities.

The management system can be extended with additional modules for formal rules verification and global security correlation [5]. It can be easily integrated with other Operations Support Services (OSS) or Service Desk applications in order to satisfy any enterprise requirements.

VI. References

1. McHugh J., - Intrusion and Intrusion Detection, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2001

2. Sandro G., Zeliko H. - Information system security threats classifications, Journal of Information and Organizational Sciences (Online) e-ISSN: 1846-9418

3. Fengying W., Caihong L., Lei Z., Xiumei L. - A comprehensive security policy research on web information system, IEEE International Conference on Automation and Logistics, ISBN: 978-1-4244-4794-7, 2009, pp.1776-1780

4. Alex X. Liu, - Formal Verification of Firewall Policies, ICC '08. IEEE International Conference on, Vol. 1, 2008, pp. 1494-1498

5. Gheorghică D. - Contribuţii la modelarea şi analiza reţelelor de comunicaţii în vederea optimizării performanţelor acestora - Managementul securităţii şi securitatea managementului în reţele IP -", PhD. thesis, Bucharest, 2010, pp. 105-120

6. M.G. Gouda, X. Liu, - Firewall design: consistency, completeness, and compactness, Distributed Computing Systems, Proceedings, 24th International Conference on, 2004. pp. 320- 327