MONITORING AND ALARM MANAGEMENT FOR SYSTEM AND NETWORK SECURITY:

A web-based comprehensive approach

João Afonso
Informatics and Systems Laboratory, Pedro Nunes Institute, Coimbra, Portugal
Email: jafonso@ipn.pt

Edmundo Monteiro
Department of Informatics Engineering, University of Coimbra, Coimbra, Portugal
Email: edmundo@dei.uc.pt

Carlos Ferreira[1]
Fisheries Inspection Department, General Direction of Fisheries and Aquiculture, Lisbon, Portugal
Email: carlosferreira@igp.pt

Keywords: System and Network Monitoring; Trouble Ticketing systems; Warning Management; Systems Administration; Internet services, Dial-up networking, bill forecasting .

Abstract: In this work we propose a computer platform that aims to unify the tasks of monitoring, diagnosing, error detection, alarm management and intrusion detection associated with the administration of a computer network and related critical services. As main objective, we intend to develop a user-intuitive program that does not require specialized computer skills from the operators in order to assume full responsibility for the system. Open-source solutions were used, whenever possible, namely for server operating systems, application development tools, database engine and integrated Web solution. The project started by studying the existing solutions, exploring their strengths and shortcomings and iteratively defining the specific requirements to be implemented. The development phase was conceptually divided in three different levels: the agents and connectors collecting the data from the different areas being monitored; the database engine, cataloguing the information and the Web Interface (Security Portal) that allows the management of all functionalities and guarantees the operationability of the solution. An alarm management tool should also be developed permitting, according to programmed warnings for certain malfunctions, trigger the warning messages through the pre-defined medium – E-Mail, SMS (short message service) or IM (instant messaging), using a Unified Messaging (UM) solution. According to the defined specifications, the solution to be implemented was designed and a functional analysis was created. Finally the projected solution was implemented and applied to a case study – the Department of Fisheries Inspection from the General-Directorate of Fisheries and Aquiculture. The preliminary results from the reliability and user-friendliness tests were very positive and a decision was made to move into the production phase. The platform was developed in line with current accessibility requirements and can be operated / consulted by users with disabilities.

[1] Currently Head of Computing Services, Santa Maria Hospital, Lisbon.

1 INTRODUCTION

Running a computer network today, regardless of size, requires a set of network equipments, several servers (possibly running on a number of different platforms/operating systems) and a large number of available services (e-mail, www, ftp, newsgroups and database engines, among others). Crucial to the work of maintaining such an infrastructure is the task of monitoring all services and equipment and subsequently directing the necessary alerts for the relevant person. The recipient of the message must be promptly informed of the occurrence regardless of being on site or not and using his/her preferred mean of communication.

Despite the extensive range of systems currently being marketed (e.g. Hewlett-Packard Openview[2], for equipment management; Quest Big Brother[3] for server and services monitoring; Remedy[4], for alarm management and system and network safety) we still lack a single solution aggregating all required functionalities. In our opinion those would have to include: intrusion detection, trouble ticket management; continuous network survey; equipment and services monitoring and predicting telephone bill for WAN networks with dialup access.

The aim of our work was to propose a solution that would integrate all these components in an easy to use Web interface, although admitting that, for the sake of simplicity, the final solution could not include the myriad of functionalities presently found in those systems.

Throughout the project we tried to use as much low cost solutions as possible. All gateways used are "no fee" systems, only SMS (Short Messaging Service) messages have to be paid according to standard mobile phone operator fees. For e-mail the option was Qmail and for instant messaging we used Jive Messenger (server)[5] and Exodus (client)[6], both respecting and implementing XMPP – Extensible Messaging and Presence Protocol (P. Saint-Andre, 2004).

In implementing the solution, we resourced as much as possible to open source solutions and free binaries implementations. In the cases where this was an option, the necessary tools had to be fully developed using a variety of platforms (Java, PHP, Jsp, etc.). That was the case of the Web portal, the telephone bill predicting system and the agents for the Windows and Unix platforms specifically developed according to the project specifications.

All developed components were implemented in compliance with the guidelines of the Web Accessibility Initiative (WAI)[7] and the Web interface was designed to be used by users with accessibility limitations.

[2] http://www.openview.hp.com
[3] http://www.quest.com/bigbrother
[4] http://www.remedy.com
[5] http://www.jivesoftware.com
[6] http://exodus.jabberstudio.org

2 SYSTEM REQUIREMENTS

The following system requirements were considered for the proposed solution:

- The existence of a relational database management system (RDBMS) capable of collecting information from all possible sources, managing all the services and permitting an easy access to the data, including cross-correlation functionalities (Figure 1);

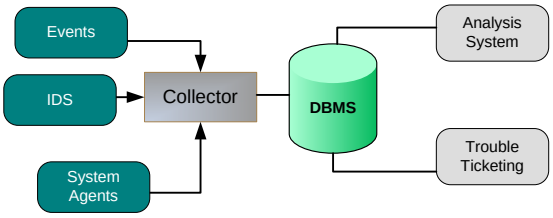

Figure 1: Interaction diagram between the agents, RDBMS and the analysis systems

- For each system to be monitored, there should be an agent, running on different platforms and operating systems. The information collected from the agents, should be periodically reported to the RDBMS, in a manner similar to the one used in Simple Network Management Protocol (Simões, 2000).
- The ability to implement a trouble ticket solution (Figure 2), capable of managing the process of sending the alerts using an integrated Unified Messaging solution compatible with the three pre-defined gateways: e-mail, SMS and Instant Messaging (IM). The system should also be capable of registering delivery confirmations, in the cases where that is possible (e.g., SMS and IM) and also saving the messages for posterior delivery when the user is offline. The alerts can be sent to internal staff of the company/institution or

[7] http://www.w3.org/WAI

to external technical support services responsible for maintaining the equipment (e.g.: Internet Service Providers, telephone companies, hardware maintenance/support companies). The system should also be able to propose a method to solve the problem, providing a user, independently of his/her experience, with a suggested route to solve a problem;

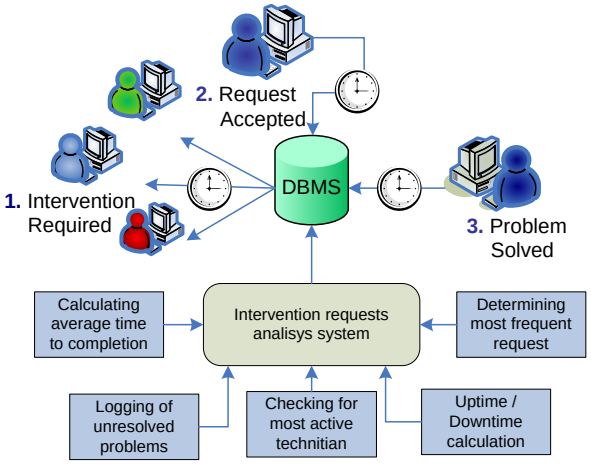

Figure 2: Trouble ticketing solution

- The capacity to incorporate intrusion detection mechanisms, capable of logging, in the database engine, the different forms of potential attacks and their origin. This information should be stored in the RDBMS, applying a set of rules and filters, so they can be easily reviewed, and correlated with other sources of information (e.g., firewall), in real time;
- The possibility to centralize in the RDBMS the logging of events processed via Syslog (Eaton, 2003). For that purpose, the different machines (servers, independently of platform, or equipments that can interact with a server, e.g., Printers, Access Points, Routers, Firewalls, etc.) should behave as Syslog clients;
- The possibility of being administered using a Web browser including tasks such as: diagnostics (including repetitive attempts to check for activity and, in case of malfunction, suggesting a way to correct the fault); production of reports in Adobe Portable Data File (PDF) format[8]; checking the log for triggered daily alarms; possibility of predicting telephone bill for dial-up connections; uptime and downtime statistics, for each server and service being monitored; Syslog sources event log; possibility to send messages to users using UM and associated available gateways; two groups of users – restricted access and administrators – with different levels of access to the system. The portal will also have back office functionality for advanced administration options (restricted users only), making possible to define witch systems and services to miniaturize and which users to contact;
- AAA (authentication, authorization and accounting) system for WAN (wide-area network) accesses (Laat, 2000). This way, the validation should use RADIUS (Remote Authentication Dial-In User Service) (Rigney, 2000) using the user data stored in the RDBMS.
- Access logging should also be located in the RDBMS, in order to detect unusually long calls, an excessive number of calls or even the absence of communication from a remote point. Can also be important to forecast the cost of communications, in advance of the phone bill.

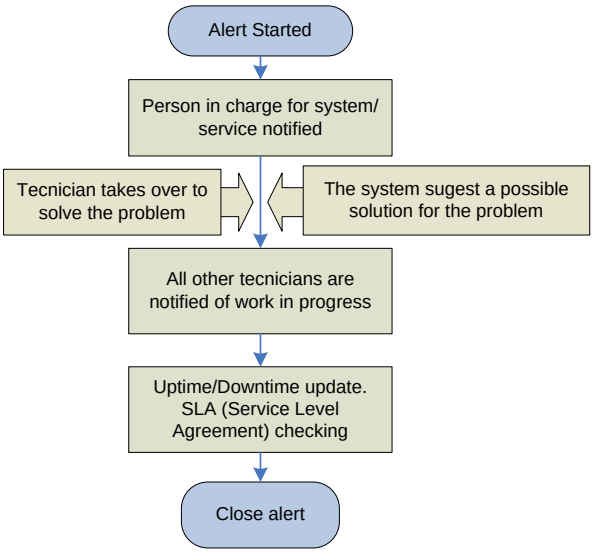

Figure 3: Alarm management

- For alert management, the possibility to implement a trouble ticket solution that could allow not only to register a malfunction but also the moment that the technician assumed

[8] http://www.adobe.com

the problem and the time that it took to solve the problem (Figure 3). Additionally, for the benefit of less experienced technicians, each alert should also include a suggested path of action to correct the problem.

- An autonomous platform has to be created to continuously analyse the data collected in RDBMS and act as necessary. There should also be automatic mechanisms available to test connectivity over the local area networks and other connections to branches offices.

3 PROPOSED SOLUTION

The proposed solution is based in cost-free applications and specially developed components. The database engine used was Mysql[9] – an open source RDBMS that uses Structured Query Language (SQL) – based on a Sun Solaris 10[10] central operative system developed for AMD platforms on a SUN Fire V20z Server.[11]

The system can handle data collected via Syslog providing the transport and storage mechanisms for event notification messages, in the form of log files, helping the administrator to classify, analyze and process from a large variety of events (according to a set of rules).

Syslog is available in Unix systems and some network components. Events are collected, according to a set of filters and rules and centralized in the RDBMS using Msyslog[12]. This application works on the same port as the Syslog protocol, directing the collected data to the database engine. In Windows systems, that lack the Syslog client, we used EventReporter[13] in order to emulate the behaviour of a Syslog client (replacing the Event Viewer).

As IDS tool, we used SNORT[14] (Caswell, 2003) – an open source platform, that works as a packet *sniffer* monitoring network traffic in real time, scrutinizing each packet closely to detect a dangerous payload or suspicious abnormality, according to a group of known signatures. The implementation is adapted to work with the RDBMS. In this way, the Web interface can be used to monitor the system, to correlate the data with other sources of information or even to generate alarms according to specific situations. It is also possible to generate alerts based on information reported by this solution.

Figure 4 shows a diagram for the proposed solution.

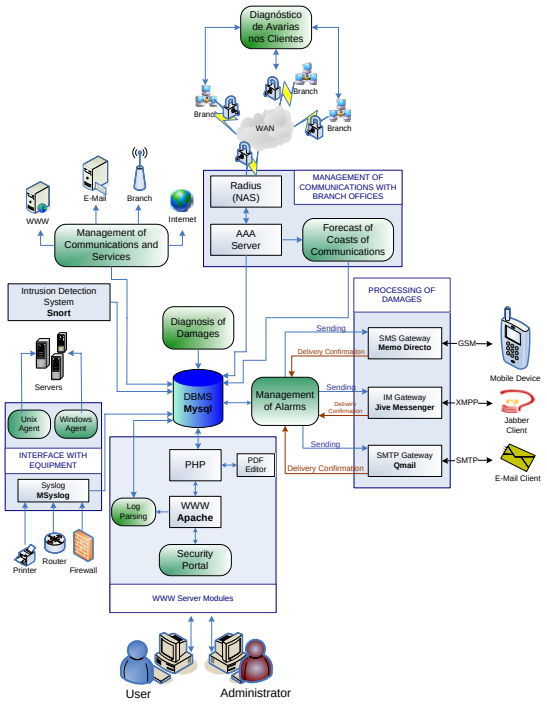

Figure 4: Overview of the proposed solution

The IM gateway was implemented in Jabber[15], (an open source initiative), Extended Markup Language (XML) using XMPP (an IM protocol) and online presence detection. On the server side, we used Jive Messenger and in the client side Exodus. A virtual user was created – MAM – monitoring and alarm management, responsible for processing the alert messages and sending them to the users (local and remote) and technical services (internal or external).

For validating the authentication, authorization and accounting operations of the remote users, we use the RADIUS protocol, also adapted to interact with the RDBMS engine. This solution is also used to predict the communication costs.

To complement the information collected a set of java agents (Unix environments) and services (Windows systems) was developed. The task of these agents is to collect system information,

[9] http://www.mysql.org
[10] http://www.sun.com/solaris
[11] http://www.sun.com/servers/entry/v20z/index.js
[12] http://www.sourceforge.net/projects/msyslog
[13] http://www.eventreporter.com
[14] http://www.snort.org
[15] http://www.jabber.org

namely disk space, memory usage and to perform service monitoring. These agents are, at the same time, sources of information for the central database engine, with which they interact on a periodic way.
Several java applications run in the background in the central system – at predefined periods of time – analyzing the information collected and running a set of diagnostic tests.
All the information is available through a Web interface, after good validation of the login/password pair and according to the profile of each user. This profile will indicate if the user has administrative rights allowing access to Back Office operations (such as: programming alerts, monitoring processes, sending messages, and managing accounts and contacts).
At the main page the user can see a briefing of all information, indicating the last events reported, the state of all communication channels, the state of the services being monitored and last IDS attacks reported.
Functions available include searching, running queries over the data, and running diagnosis to determine possible problems.
In the Back Office section, an administrator can use options such as management of users and external contacts, defining areas to supervise and programming of alarms.
An important feature of the system is that the data can be analysed *per se* or correlated within a certain time frame. This option can be very useful, for example, in the cross-evaluation of information obtained by the IDS solution and the Firewall (Shearer, A., 2003).

The settings for the different alerts and the corresponding users and contacts that are notified can also be defined using the portal. The Web interface is also used to define the different areas to be monitored, indicating which equipment and services should be checked and with which periodicity.

The WWW server is based on Apache[16] technology, and the application development was done in PHP[17] (Rehman, 2003).

The integration of the different technologies, together with the tools created is presented on Figure 5.

[16] http://www.apache.org
[17] http://www.php.org

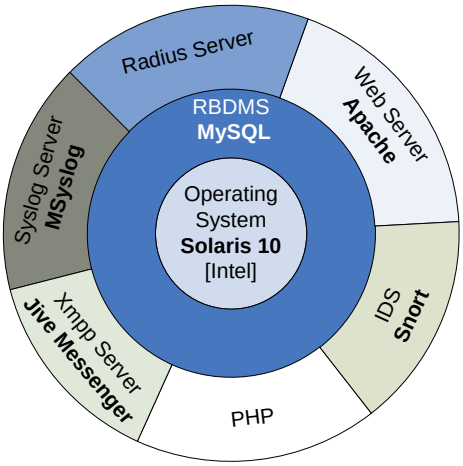

Figure 5: Diagram of the technology used

The global solution is platform independent so the technologies we used can be easily exchanged by others that respect the same functionality: the RDBMS MySQL could be replaced by PostgreSQL[18], Oracle[19] or SqlServer[20]; the Web server Apache could be replaced by Internet Information Services[21] or other and for the IM solution, Jabber client (Exodus) and server (Jive Messenger) could be replaced by Rhombus[22] for the server side and Gush[23] or Trillian[24] for the client side.

4 CASE STUDY

The Portuguese General Directorate of Fisheries and Aquiculture[25], with a total of 97 branches and a complex web of local networks - all considered critical and, consequently, in need of close monitoring - was chosen for an initial implementation of the proposed solution.

[18] http://www.postgresql.org
[19] http://www.oracle.com
[20] http://www.microsoft.com/sql
[21] http://www.microsoft.com/iis
[22] http://www.rhombusim.com/
[23] http://2entwine.com/
[24] http://www.ceruleanstudios.com/
[25] http://www.igp.pt

Figure 6 shows a snapshot of the Security Portal.

Figure 6: Security Portal – Global overview

All the information available at this page is generate from the RDBMS. The main portion of the window shows all the critical information regarding the communications and services being monitored.
The information available, concerns events, recent alarms triggered, and top IDS attacks detected.
The left panel shows the options menu. Functionality depends on user privileges (administrators can access the *back office* options).
In the right panel users can access the query tools to search in the repository of data (from alerts, events and IDS solution). The search can be done by date limits, server or part of the text used in description.

In Figure 7, we present a diagram of the systems involved in the solution proposed for the Directorate.

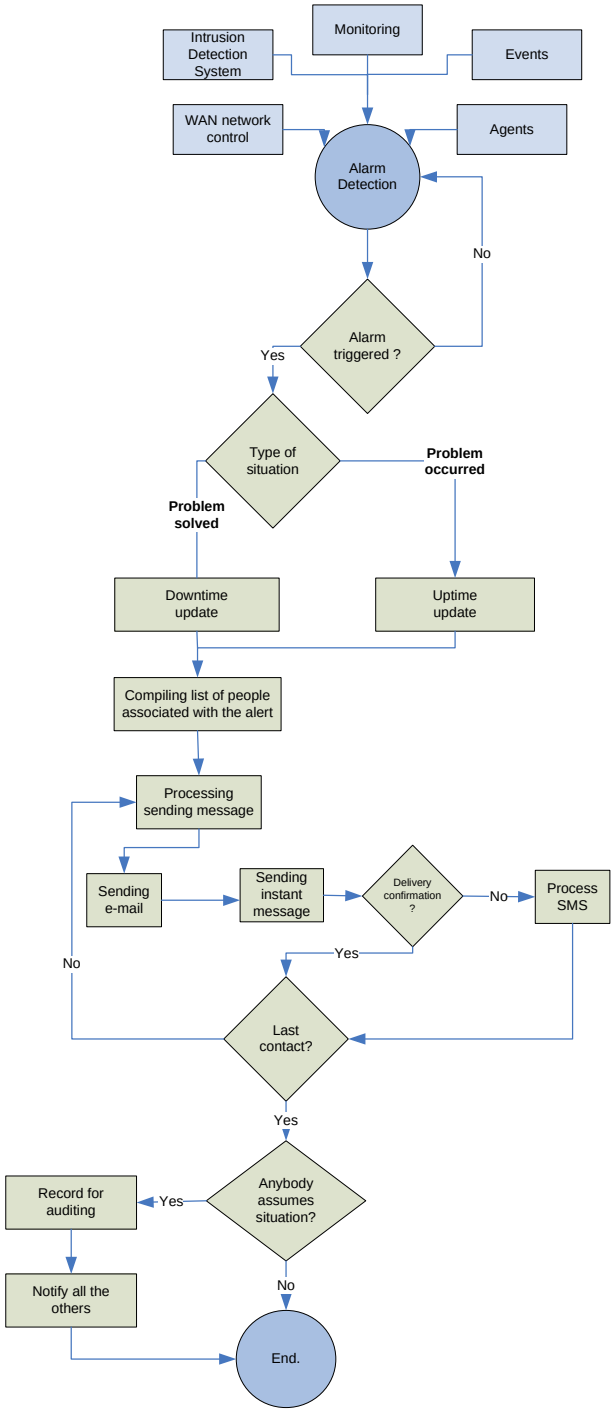

Figure 7: General diagram of the solution implemented in the case study

In total, there are five information sources feeding the database engine: Intrusion detection system, WAN network control, system monitoring, events

(Syslog and Eventreporter) and agents (specifically developed for Unix and Windows environments).
To insure that the Web interface is in compliance with the Web Content Accessibility Guidelines (WCAG), the interface have been tested with Bobby[26] – accessibility desktop testing tool.

5 PRESENTATION OF RESULTS

The proposed solution is currently being used in the Portuguese General Directorate of Fisheries and Aquiculture and initial results are very positive.
As an example we present below the principal indicators for the first two months of functioning in the period between 1/10/2004 and 30/11/2004, collected from the different sources:

Table 1: Main indicators for the initial 2-month period

IDS	Events	Alarms	Radius
45000	776163	147	119885

In addition, a total of 5380 SPAM messages, 974 virus containing e-mail attachments, 354 alerts from WAN network and 28 message alerts on local equipment and service failure where also reported during this period.

The high Radius value, reflects the large number of calls between the branches and central office, over the dial-up ISDN channels.

Figure 8 presents the top 10 possible attacks detected by IDS.

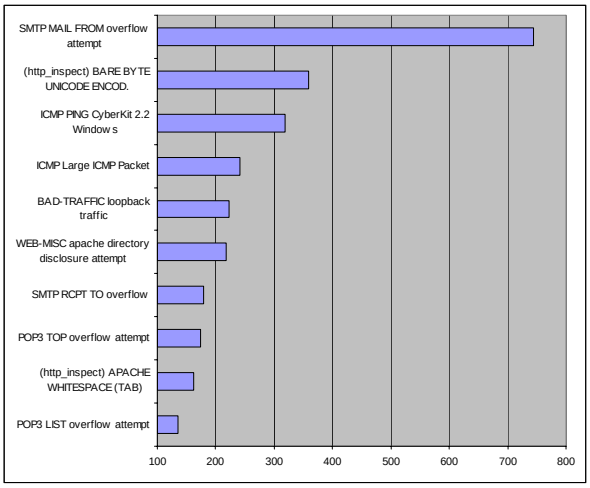

Figure 8: IDS – attacks sorted by number of occurrences

The number of IDS events reported can be minimized by using appropriate IDS rules to classify false positive alerts – that can be used maliciously by an intruder to start a massive attack, obfuscating small events that could be undetected. Also false negative alerts can be avoided, when the analysis system correlate events reported by IDS with other sources – firewall, syslog agents, etc – in the same time frame (Gerg, 2004).
There are currently a total of 30 internal users (with access to the security portal) and 70 external contacts (that can be informed about problems related with the systems under their administration).

6 CONCLUSIONS AND FUTURE WORK

With the proposed solution we have been able to administrate a total of 97 branches, over 30 servers running distinct services such as database engines, e-mail, proxy, newsgroups and many others. A set of analysis agents were developed that continuously monitor the information collected in the RDBMS and trigger the corresponding alarms according with a pre-defined set of rules. A Web portal is also available that permits users to view all the information, create reports and manage the way alerts are triggered and distinct areas should be monitored. A set of diagnostic tests is also available and, since all reports include a clear path towards a possible solution, the user does not need be an expert to solve the problems.

[26] http://www.cast.org/bobby

The solution had a considerable impact in the efficiency of the monitored services notably in reducing service downtime, improved security, and increased efficiency of the technical staff as well as a substantial reduction in communication costs.

In summary, the proposed solution aims to combine in a single platform the main features that are present in programs as diverse as service monitoring systems, IDS, trouble ticketing and AAA. Additionally, the use of a common RDBMS for data collection provides an easy way to analyze and correlate data from different sources therefore improving the detection and management of critical conditions. Also considered important is the inclusion of a trouble ticketing solution, capable not only of managing events but also of suggesting solutions for most common errors and problems.

The availability of agents capable to operate in several operating systems provides the necessary independence to the platform and the ease-of-use provided by the web portal developed in line with current accessibility requirements stands out from the other existing options.

The operational logic, assigning services, equipments or even entire areas to a network of responsible technicians promotes accountability and improves the overall performance of the maintenance.

Future work planned includes the expansion of the portal to allow GSM (Global System for Mobile Communications)/PDA (Personal Digital Assistant) access. This way a user could send commands and receive reports using a mobile terminal (Figure 9, on the left).

Another interesting addition would to integrate an IP camera solution to the system that would notify the security company and create a VPN (Virtual Private Network) allowing access to the images (Figure 9, on the right).

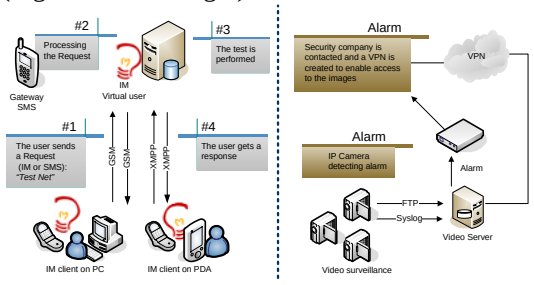

Figure 9: Possible future development with two-way interaction with mobile terminals

7 REFERENCES

Caswell, B., Beale, J., Foster, J., Faircloth, J., 2003. *Snort 2.0 Intrusion Detection*, Syngress.

Eaton, I., 2003. *The Ins and Outs of System Logging Using Syslog*. SANS Institute.

Gerg, C., Cox, K., 2004. *Managing Security with Snort and IDS Tools*, O'Reilly.

Laat, C., Gross, G., Gommans, L. Vollbrecht, J., 2000. *Generic AAA Architecture*, RFC 2903.

Lonvick, C., The BSD syslog Protocol. RFC 3164.

P. Saint-Andre, Ed., 2004. *Extensible Messaging and Presence Protocol (XMPP): Core*, RFC 3920.

P. Saint-Andre, Ed., 2004. *Extensible Messaging and Presence Protocol (XMPP): Instant messagind and presence*, RFC 3921.

Rehman, R., 2003. *Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP ad ACID*. Prentice Hall.

Rigney, C., Rubens, A., Simpson, W. and S. Willens, 2000. *Remote Authentication Dial In User Service (RADIUS)*, RFC 2865.

Rigney, C., 2000. *RADIUS Accounting*, RFC 2866.

Shearer, A., 2003. *Firewall log analysis using ACID*. SANS Institute.

Simões, P., 2000. *Gestão distribuída de Redes Baseada em Tecnologia de Agentes Móveis.* Universidade de Coimbra.

Strebe, M. et al, 2002. *Firewalls 24Seven*, second edition. San Francisco: Sybex.