Global Information Assurance Certification Paper

Security Management

Practical Assignment Version: 1.4b
Option 1

Adam Wojnicki
6th of January 2003

Abstract

This paper is a big picture of security management. Three major issues are discussed: centralized management of the security policy, monitoring of the security devices as well as log analysis and reporting.
It also presents state-of-the-art solutions available on the market covering the above security management needs. It compares available products indicating what features to look for.

Introduction

"One of the toughest jobs for information security professionals is getting real-time information about what's actually happening across their company networks. While many security tools such as firewalls, intrusion-detection, and anti-virus software come equipped with their own management consoles, none provides a single view of events along the network perimeter, such as attempts to crack into the corporate server and a listing of viruses that are infecting the E-mail system."[1]

Sometimes we think that an Information System is secure because it is protected by the most up-to-date products available on the market: high performance perimeter firewalls process connections coming from the outside world, the intrusion detection system is checking the local network for potential threats, and all operating systems are hardened. However, there might be still something missing.
The administrators spend hours on implementing the security policy going from one firewall console to another, as more firewalls from different vendors were chosen by a security measure. What if they omit to close a telnet connection to an important server just because the firewall rule-set is too complex?
Analyzing firewall logs is such a nightmare that people are just not doing that at all. Security alerts are raised, but given the number of managed systems, people never see these alerts. Security simply relies then on confidence put in security of chosen products and not on the real knowledge of what is happening in the Information System.
If the above situation sounds familiar to you, then you definitely need to improve the management of your security. A central alert console will help you see on one single screen what all your security equipments are detecting. From now on you will be aware of all connections dropped by the firewall. Log analysis utility will warn you when it detects a long period scan and provide you with a daily report on most-aggressive sources from the Internet. The security policy administration tool will help you to centrally declare all permitted flows.

Never forget the following: one thing is to be able to detect an intrusion, another thing is actually to be informed about that fact. This is especially true for big and highly heterogeneous environments such as, for example: banks, hosting

platforms. Operation teams are often flooded by information and without a specific tool it is difficult to see when something bad happens.

What is involved in security?

Managing the security of large security architecture may be very complex. Let's take for an example a secured Internet access. The connection may be as follows: once the user is authenticated by the authentication server, the connection is forwarded to the anti-virus software, then to the content filter and finally it will pass through a firewall. This is just an example, but already it gives an idea of the complexity of security devices' management. Think about log analysis. You will have to correlate the logs coming from all of the above equipment in order to know where did the intruder came from.

Usually the security relies on some or all of the following types of security equipment:

- Firewalls
- Routers (ACL, log in and out) and switches
- Authentication servers
- Flow encryption
- Scanners vulnerabilities
- Host-based IDS
- Network-based IDS
- Web servers
- Content security and anti-viruses
- Operating Systems
- Load balancing equipment

All of these equipments are very important. The general guideline, while taking into consideration security management solutions, is to choose the solution that will cover as much as possible from the above list. If a policy management tool can cover many different types of firewalls you effectively can manage all your equipment from one single point with coherent rules applied everywhere. Having all these equipment send their alarms to a single console will give you the opportunity to real-time correlate the information coming from different sources and have a better vision of what is actually going on. In the same time the correlation can be used for a posteriori log analysis if you have a single area for the log storage

Basic technologies

Two important protocols are used by management tools: syslog and SNMP. Even if some devices use more advanced and secure protocols, for example Checkpoint uses LEA; these two are the most widely used.

Syslog[10] is a simple way of sending logs to another host called log server. Network devices and UNIX systems use it. The messages are sent in text format,

this way they can be easily interpreted by a human. A syslog client can be configured to choose the log destination depending on type of message (facility) and associated severity.
Syslog is a one-way spontaneous communication. The messages are sent in plain text. Be careful while using this protocol, syslog messages may contain sensitive data.

SNMP[11] is different. Messages are sent in a form of OID (object identifiers) with associated values. All OIDs are defined in databases called MIB. MIBs are files explaining the meaning of OIDs.
SNMP traps are messages spontaneously sent by a device if critical condition happens. SNMP "get" and "set" can be used to interactively manage a device. Get is used to ask the device for a value of a specific parameter, set to associate a specific value to a parameter.
SNMP messages are difficult to understand for a human as they contain OID that need first to be translated to text messages.

Security policy management

Two major aspects can be distinguished in security policy management: user accounts management and flow management. We only focus on flow management here below.
In complex security architecture a simple firewall management console is not enough. Security policy can be enforced on equipment coming from different vendors; a consistency of rules through these various equipments is necessary. The needs of security policy administration are the following:

- Global flow declaration from a single point. Be able to declare an information flow for whole security architecture and not on an equipment-by-equipment basis.
- Centralized management of authentication and access control
- Management of security policy lifecycle: versioning and change management. A repository is highly recommended. A repository containing all versions of previously used security rules is very useful when doing a posteriori analysis.
- Capability of integrity check of security rules: repository vs. deployed rules

Very few solutions are available on the market to answer the need of global flow management. Solsoft offers an interesting product called Solsoft Distributed NP[2].
Solsoft NP is a visually oriented solution for managing network security. It helps design, distribute and enforce security and VPN policies across an entire network in a mulit-vendor environment. Using Solsoft NP helps focus on global policies rather than device configurations.
Solsoft NP is composed of a java-based Policy Definition Tool used to graphically define the security policy. Once the rules defined the Network Policy Engine automatically calculates, generates, validates and deploys the policies. It takes into account the network topology and the capabilities of all security devices.

Pros:

- Visual design
- Global flow declaration
- Manages users and groups with concurrent access
- A project manager is associated to every policy and can delegate rights to other users
- Workflow management
- Versioning with unlimited rollback
- Leading Firewall / VPN and Access Control supported
- Integration with HP OV/ITO

Cons:

- List of supported devices still limited
- Limited to flow management

Monitoring and management

A monitoring tool is basically a console used to display messages sent to it. This is a central point where security alerts generated by the managed security equipment can be watched. Of course a management console of a firewall can also be used to monitor these alerts. Even the alerts coming from numerous firewalls can be centralized on a single management station. But what if dozens of firewalls have to be managed and if they come from different vendors?

A monitoring tool can also do some kind of "intelligent" treatment of alerts. The received message can be interpreted in order to give to it the appropriate meaning and importance, as defined by the management policy. For instance a disk failure on a firewall might be more important then a simple link-down on a switch used by roaming users when they come to the office. Typically a system of colors is used to distinguish between various levels of severity, for example red for critical alerts, purple for information messages.
Another important function is the de-duplication. It is preferable to increment a counter if a message is repeated several times rather than display the same message many times. Sometimes alerts are generated hundreds of times per minute.
Finally alarm correlation is an important feature. This is the ability of the management console to cancel an alert if another message received later cancels the first one.

Once you have a centralized monitoring console you can organize the operation team to work with it. The organizations often use a standard 3-level helpdesk model for this purpose. First level helpdesk employees, usually called "operators", work directly with the monitoring console. They solve typical problems and if necessary contact the second level: administrators.
To solve the typical problems they use tools, which can be integrated into the management console. As an example a Checkpoint management console has a

utility to block a particular connection if an alarm is raised for this connection. A good management console should have this functionality to configure tools giving you the ability to execute them for a particular alarm.

What do you need to cover?
Most of the security products, like firewalls or IDS are actually applications running on a PC or a server. Only some network equipment (routers) are purely hardware based appliances. Therefore you should not only be able to cover application specific alarms, like for example a dropped connection according to the security policy, but also the system and the hardware alarms. These are usually not covered at all by the management consoles provided by the application vendor. However these alarms are also very important for the overall security. A broken power supply can make your firewall unavailable. A full system partition can crash your system.

Many different ways of communication can be used between the device and the management console. Some devices use syslog to send alarms, others SNMP. Some can even use a proprietary encrypted communication, for example Checkpoint uses LEA protocol.
While choosing a management console it is important to check what security devices can be managed by the tool. It is impossible to find a product, which covers all imaginable devices. An important future to look for is the ability of the console to communicate using all of the above protocols, the minimum being syslog and SNMP. The console should then offer the opportunity to self-define a rule-set used to interpret alarms and give them the appropriate importance.

Another important feature of a management tool is the ability to keep track of some system parameters. For example it is very useful to know what is the baseline for the CPU of a firewall, how often the picks appear and how long they persist.

The ability to define metrics for SLA may be important when SLA contracts should be considered. Once SLA metrics are defined, the monitoring tool will advise you through an alarm when the defined service levels are not respected.

Last but not least is the ability to do some "intelligent" correlation of events. The alerts sent by a firewall can be correlated with an authentication logs and IDS events in order to raise an alarm if a suspicious activity has been detected. A good monitoring tool enables definition of rules used to decide when an alarm should be raised.

Now that we know what are the needs, let's look closer on the solutions available on the market. What features they provide. We will focus here below on two products:

- Netcool for security management[3] from Micromuse
- BMC Patrol[45] from BMC Software

Micromuse's Netcool is a suite of monitoring products. Widely used to manage network and telco equipment.
Netcool for security management[3] is a package of NetCool products tailored for security management. The package is composed of:

- Object server: the alarms database; responsible for correlation and de-duplication of alarms. Automations can also be defined.
- Webtop: web based console client. Displays lists of alarms and maps
- Impact server: the "intelligent" component. Can define rules used to insert new alarms to the base, can send requests to external databases. It can be used to correlate messages sent by different equipment composing a secure architecture
- Reporter gateway used to synchronize events with a reporting data-warehouse
- Probes for Firewall-1, Cisco PIX, Cisco IDS for acquisition of data coming from these devices
- Syslog and SNMP probes to adapt the console to other equipment
- Can integrate with Netscreen's GlobalPRO, NA Sniffer Distributed, NIKSUN NetDetector.

Netcool is very flexible. With rules defining data acquisition and formatting of messages you can do almost whatever you want with incoming messages. However, many security products use specific protocols and you might not be able to send their events to the event base if the protocol is something different than Syslog, SNMP or OPSEC LEA.
The events can also be managed once in the alerts database. You can define rules to correlate messages. If a connection is dropped by a firewall you may want to check if it was previously authorized by the authentication service.
Display features are very rich. You can use maps with color icons, links, histograms etc. You can integrate tools into the console to facilitate the most common actions. For example "ping" command can be used as a tool integrated into the console.

Pros:

- Alarm formatting and filtering according to a rule-set defined for each probe; alarms correlation, alarm de-duplication
- Numerous probes (over 300) are available, but few of them are adapted to security management needs
- Syslog and SNMP probes with configurable rule-sets defining message interpretation can be configured for equipment supporting these protocols
- Modules available for FW-1, Cisco PIX and Cisco IDS
- NetCool/Reporter: a reporting solution is available
- NetCool/Impact to intelligently correlate alarms issued by different equipments
- Many system tools can be configured to work with NetCool. Probes exist for BMC Patrol, HP OV ITO, IBM Tivoli, NetIQ AppManager.

- Tools can be easily integrated into the console

Cons:

- No probes / monitors exists for hardware and system management. A separate tool has to be used. Exceptions to that are unix / linux systems which send events via syslog.
- Only Checkpoint, Cisco PIX and Netscreen firewalls are supported at the moment. More specific security software is not supported. The exception is Cisco IDS.
- No tracking of system parameters and performance. Netcool/Reporter can be used for reporting, however the reports are based on events received by the console and not on user-defined metrics.
- Alarm console and not a monitoring tool. No metrics or thresholds can be defined.

BMC Patrol is a suite of management tools. It is often used for system management purposes. It is composed of a console, agents and Knowledge Modules (KM). Agents exist for various operating systems: Unix, Linux and Windows. BMC also provides DBMS and application specific agents.
For the security management purposes two firewall specific agents are available: Patrol for Checkpoint FW-1[4] and Patrol for CiscoSecure PIX Firewall[5]. Using these agents together with operating system agents you can build a complete management solution. Furthermore Patrol can connect hardware agents of other vendors, for example Compaq Insight Manager or Dell Open Manage.

Pros:

- Integration of hardware monitoring and fault management
- System monitoring agents
- Specific agents for FW-1 and Checkpoint with the ability not only to capture events but also provide history of measures
- Metrics history and events history
- KM scripts and configurable thresholds for events generation
- SLA metrics and SLA events
- Corrective actions can be configured
- De-duplication and simple correlation of events (problem / problem solved)

Cons:

- Many of security applications are not covered
- No generic agents exist for Syslog, SNMP
- No intelligent correlation of events from different equipments

BMC software and Micromuse are real giants of management market. Other smaller vendors also offer security management consoles. An interesting product called Arcsight[6], covering many security devices, mixes security management console with log analysis functionalities.

Log analysis

Why is it important to collect and analyze logs?
"Failure to enable the necessary data collection mechanisms will greatly weaken or eliminate your ability to detect suspicious behavior and intrusion attempts and to determine whether or not such attempts succeeded.
Failure to configure and secure the volume of data produced by these mechanisms will place the data at risk of compromise and make subsequent review and analysis difficult, if not impossible." [9]

Log analysis is something different from real-time monitoring. Often the log analysis tool will capture the same messages as those sent to the management console. However instead of displaying them on a console, it will store the data in a central database.
Management console is for real time management. It captures events, interprets them according to the defined rules, tries correlate them to the events coming from different sources, prioritizes and finally displays them on a console.
Log analysis tool captures the messages sent by equipment. These messages are then interpreted in order to extract the useful information and adapt it to a database storage format. Then the data is inserted to the database and indexed.
One big difference between management console and log analysis is the volume of data. The objective of a management console is to keep only the relevant data and to minimize the number of messages displayed, this to bring only the most pertinent information to the end-user, which is an operation center technician.
Log analysis tool, however, is designed to store as much information as possible in its central storage, for example a database. The objective is to have as much information as possible. The data, such as communications accepted by a firewall, will then be stored and available for queries, while in case of a management console some data may be suppressed as soon as received if judged irrelevant. For a log analysis solution you may want to store as much as a year of logs, or even more.
While for the management consoles the data is displayed on the console's screen and seen by operators, log analysis data is stored in a database and consulted through queries.

Log analysis tools help also detect long-period intrusion attempts. Without log analysis somebody could do a scan of ports testing just 1 or 2 ports per day and never be detected.
The important functionality of a log analysis tool is to provide the management with security reports and dashboards. For example a report classifying network domains per number of refused connections can be created.

The main features that should be researched are the following:

- Automatic acquisition and centralization of logs. Security devices use various means of log storage. Some of them simply write logs to a file, others send it using Syslog or an encrypted protocol. For log analysis purposes a support of all of these protocols and formats is necessary.

- Secure storage of logs. Logs may contain very sensitive data, for example dropped connections, authentication information such as usernames. For security reasons this is very important to store this information in a secure way.
- Log analysis through queries with flexible criteria
- Cross-analysis of logs from different security equipments
- Pre-defined reports and dashboards
- Good performance and pertinent design of data storage component as some queries may take hours or days to execute.

Still very few solutions exist on the market. Historically people used scripts for log analysis purpose. This can be a good idea if a batch execution can be programmed for example every evening and if the reports are well defined and not changing too often. This kind of solutions is however hardly maintainable. Furthermore the data storage in a file format is a real issue if the data represents Giga or Terrabytes. Actually, an indexing system is necessary.
And what if you find out that an intrusion occurred and you want a report on all connections coming from a particular source during the year proceeding the day the intrusion was discovered? Will you spend few days on developing a script while the management is waiting for a quick answer?
For these reasons a solution based on a database is necessary.

One of the solutions available on the market is NetsecureLog[7] from Netsecure software.
The solution is composed of the following components:

- An "external agent" used for data acquisition. This component is either installed on the equipment you want the log to be centralized on or on a different server playing the role of a Syslog server.
- An "Internal Agent" responsible of data acquisition and storage in the database
- A Database storing the data and executing the queries
- An "Analysis agent" accessible with a web browser used to launch the queries and see their results.

Pros:

- Good coverage of security equipment, including the following: firewalls, routers, authentication servers, anti-viruses, web servers, proxies, network and host-based IDS, operating systems and others.
- Support of numerous log formats and protocols
- Central storage of data in a database using a uniform data format
- Web-based access
- Security of all communications
- Flexible data consultation through queries
- Correlation of logs coming from various equipment
- Basic pre-defined reports available

- "Real-time" monitoring functionalities: alerts can be generated according to defined conditions

Cons:

- Some important equipment not supported, for example not all of IIS server file formats are supported
- Agents have in some cases to be installed on the security equipment. Security risks need to be evaluated.
- A data warehouse could be used for storage instead of a simple database. This would give better performance.

NetForensics[8] is another interesting log analysis tool, which should be considered while choosing a log analysis solution. NetForensics Universal Agent uses a XML file to define rules of log file interpretation. This way any event source can easily be incorporated to the correlation engine.

Security of management tools

Another important point to consider while looking for management tools system is the security of the tool itself. If the logs are stored encrypted on the firewall but their transfer to the log analysis tool is not encrypted, then the security is compromised.

Here below are some important features to look for:

- The access to the tool should be restricted by a username / password
- It should be possible to give specific rights on a per user basis
- If the tool is web based, the traffic web browser – web server should be secure. Check if HTTPS is supported
- The transfer of the information should be secure. Check what protocols are used
- The information should be stored securely
- All changes and connections should be logged.

Some protocols transfer the information in an unencrypted way, for example Syslog. This can be very dangerous, as messages often contain sensitive information. This can be a username of the user not successfully authenticated by the system.

Using SNMP can also be very dangerous if improperly configured. One could use SNMP to reboot a server for example. Pay a careful attention to SNMP configuration. Do not forget to change the default community values.

Conclusion

Information security is a critical issue for many organizations today. Number of security devices to manage is increasing, as security architectures are more and more complex. Good security is built using multi-vendor equipments. Managing such a heterogeneous environment is often a nightmare. Without good

management tools it is impossible to control the situation and know if the security of data is ensured.

Security management is very complex. Many aspects need to be taken into account. This article focused on three major aspects of security management: policy enforcement and management, security monitoring and log analysis and correlation. State-of-the-art solutions available on the market were presented with a brief discussion of pros and cons.

Keep in mind that to be sure that an information system is efficiently protected you not only need the best security devices available on the market, but you also need to check if everything is working as planned. In a complex environment the only way to do that is to use adapted security management tools.

Bibliography

1. Hulme, George V. "Centralized Security Management On The Way" URL: http://www.informationweek.com/839/security.htm (May 28, 2001)

2. "Solsoft Distributed NP", product information at Solsoft's homepage URL:http://www.solsoft.com/solsoft.cfm?pageid=132 (Jan 10, 2003)

3. "Netcool for Security Management", Micromuse homepage http://www.micromuse.com/downloads/pdf_lit/netcoolforsecurity.pdf (Jan 10, 2003)

4. "Patrol for Checkpoint FW-1", BMC Software homepage URL:http://www.bmc.com/products/proddocview/0,2832,19052_19453_23326_7072,00.html (Jan 10, 2003)

5. "Patrol for CiscoSecure PIX Firewall", BMC Software homepage URL:http://www.bmc.com/products/proddocview/0,2832,19052_19453_23317_7674,00.html (Jan 10, 2003)

6. ArcSight, ArcSight homepage, URL:http://www.arcsight.com/product.htm (Jan 10, 2003)

7. NetsecureLog, Netsecure Software homepage, URL:http://www.netsecuresoftware.com/netsecurenew/Products/NetSecure_Log/netsecure_log.html (Jan 10, 2003)

8. NetForensics, NetForensics homepage, URL:http://www.netforensics.com/netForensics.html (Jan 10, 2003)

9. CERT security practices, CERT homepage, URL:http://www.cert.org/security-improvement/practices/p092.html (Jan 10, 2003)

10. "The BSD syslog protocol", IETF homepage,
URL:http://www.ietf.org/rfc/rfc3164.txt (August 2001)

11. "The Simple Network Management Protocol", IETF homepage,
URL:http://www.ietf.org/rfc/rfc1157.txt (May 1990)

Last Updated: July 26th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event