Securing the Organization with Network Behavior Analysis

Jack TIMOFTE
Praktiker Romania

To protect from the ever-growing number of security threats, organizations are looking to implement more and more sophisticated security solutions. This is a normal path, since the traditional means of protecting the enterprise, by using firewalls, cannot offer the desired protection level. Tools like intrusion detection systems and intrusion prevention systems are such examples. Another such technology is the Network Behavior Analysis (NBA), which can be implemented as a stand-alone system or included in IDS/IPS or other security tools. The article outlines the NBA technology with its features and limitations and presents the current situation and the possible uses of this technology.
***Keywords**: Network security, NBA, network behavior analysis, network monitoring.*

Introduction

Network Behavior Analysis, or shortly, NBA, was initially designed as a security technology whose purpose is to identify unusual traffic on the network being supervised. An NBA system works by identifying unusual traffic patterns which can include different attacks like Denial-of-Service, policy violations, trojans or worms. NBA can be implemented using hardware appliances or it can be available as software package. The traffic flows, which are the primary data for the NBA analysis, are usually gathered directly by sensors (also known as analyzers) or provided by routers or other networking devices in a traffic flow data format. There are several standards for flow data formats, the most used being NetFlow and sFlow.

Architecture of an NBA system

The implementation of an Network Behavior Analysis system in an organization can be made as a separate management network or as part of the organization's standard network.

An NBA system has sensors and consoles, the sensors usually being hardware appliances. The following figure illustrates such an architecture, in which the NBA sensors collect the data from the switches. Like in an intrusion prevention system (IPS), an NBA sensor can be passive or inline depending on the point where it resides on the network. An inline sensor is deployed so that the network traffic it is monitoring must pass through it, similar to a firewall. Actually in some combined NBA/IPS products the NBA sensor can have IPS or firewall functions. An NBA passive sensor gets the data from a router or switch, like in the example below.

Capabilities and Limitations of NBA

Based on the traffic flows, the NBA systems can generate and maintain list of hosts communicating on the organization's monitored networks. Usually, for security analysis, the system records the source and destination addresses, source and destination TCP or UDP ports, ICMP type codes, number of packets and bytes per session, timestamps etc. Based on this primary information, the system can monitor port usage, perform passive fingerprinting or use other techniques to gather detailed information on the hosts. The hosts can be identified as a record of the IP address, operating system, the services provided (for example http or telnet), other hosts which it communicates with, what services it uses and which IP protocols and TCP or UDP ports it contacts on each host. Then, any change to the 'normal' behavior can be detected and reported.

But how is determined the 'normal' behavior? Most products rely on the use of a technique called anomaly-based detection, which means that the system can 'learn' the normal behavior patterns and then identify any deviation from these patterns. For example, a workstation normally accesses the intranet, e-mail and file servers. This is called the 'nor-

mal' behavior of that workstation. So when the NBA system identifies that there are traffic flows initiated from this workstation directly to other hosts on the network (for example a port scan of other hosts, or a connection to the telnet port of the router), it can trigger an event.

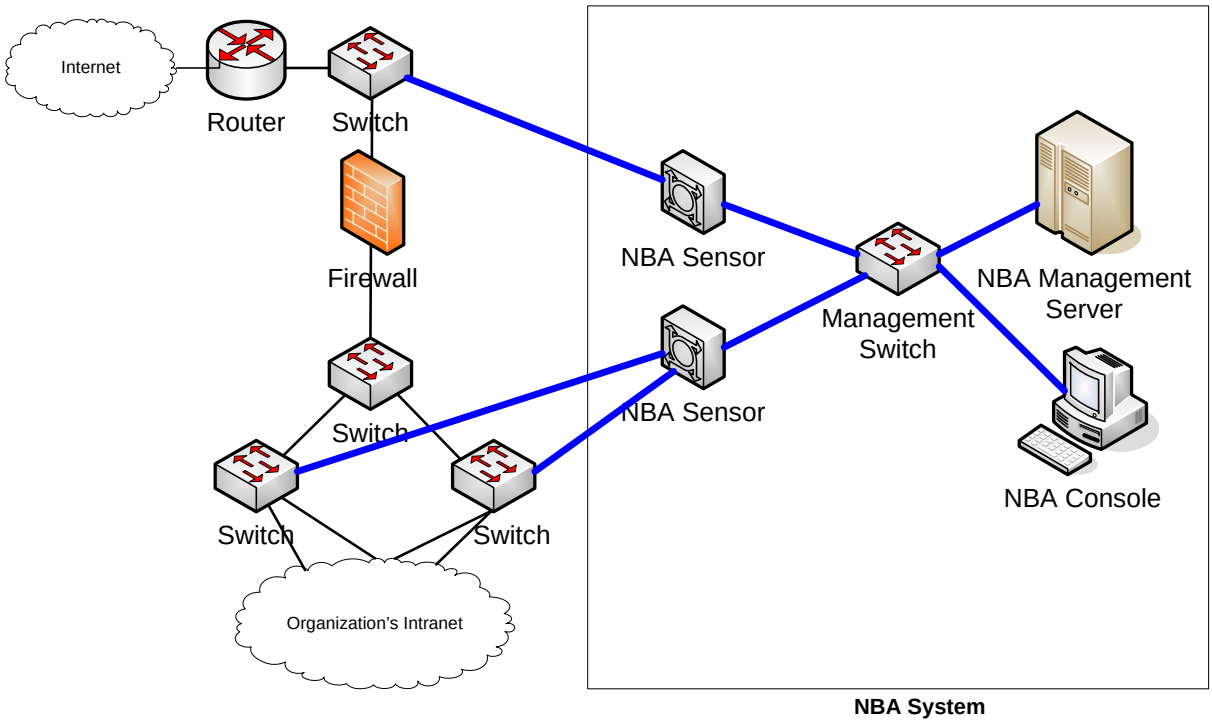

Fig.1. Example of an NBA system architecture

The normal behavior is usually set through a learning process: the system is constructing the traffic patterns which identify the normal use by analyzing the existing traffic for a specific period of time. Some NBA systems also allow the administrators to also define manually custom rules in order to detect specific threats.

All the systems usually have a monitoring console, which allow the administrators to maintain the system and monitor the network, and various notification systems can be used (e-mail, pager, SMS etc)

Types of Events Detected. Generally, this includes Denial of Service attacks, scanning, worms, unexpected services. The system can also be implemented to monitor policy compliance and detect policy violations.

The Denial of Service attacks, including distributed denial of service (DDoS) attacks involve a highly increased network traffic originating from or to a certain host, which usually has a different traffic profile. This attack can be detected using the anomaly-based detection technique, but some NBA systems are aware of the characteristic of common denial of service tools and methods, and can recognize the threats more quickly and prioritize them more accurately.

The network scanning can be detected by atypical flow patterns originating from a host. This can occur at the network layer (such as ICMP scanning), transport layer (TCP and UDP port scanning) and application layer (such as banner grabbing).

For the detection of worms there are several mechanisms based on bandwidth usage, two-way communication between hosts, the use of normally inactive ports or the use of network scanning (activities which are usually performed by many worms).

Unexpected application services include tunneled protocols, backdoors, the use of forbidden application protocols and are detected by stateful protocol analysis.

As we mentioned, a network behavior analysis system can also detect policy violations. In order to use this feature, the administrators must specify detailed policies regarding the hosts or systems being monitored. These policies usually contain information like hosts which can be contacted, which types of activity is permitted and during which periods of time (for example the activity is allowed only during the working hours), which ports are normally open etc.

The limitations of NBA systems usually derive from the anomaly-based detection. While the detection of events which include a large amount of network activity is pretty accurate, some small-scale attacks, especially if they are conducted slowly and do not violate the administrator-set policies can remain undetected. The detection accuracy in anomaly-based technology also varies over time, since the NBA system cannot detect many attacks until they reach a point where their activity is significantly different from what is considered 'normal'. For example, a denial-of-service attack which starts slowly and increase in volume over time is usually detected by the NBA system but the point of detection may vary considerably between different NBA products.

Another problem are 'false positives', like in the case of intrusion detection/prevention systems. A 'false positive' occurs when a legitimate activity is detected as anomalous by the Network Behavior Analysis system. Setting the NBA system to be more sensitive to anomalous activity may considerably increase the number of false positives. A false positive can also be generated by changes in the environment, such as a new service which is implemented legitimately and implies opening additional ports on some hosts.

Another limitation comes from the performance of such a system, since the NBA sensors have to deal with very large volumes of traffic data.

The delay in the anomaly detection can represent a problem as well. Delay can be introduced not only by the algorithm, but also by the data sources, since often data from other devices is transferred to the NBA system in batches. Depending on the product's capabilities, network capacity and settings, the transfer of batches can occur relatively frequently (every few minutes) or relatively infrequently (e.g. every 30 minutes). This can be a real problem in the case of fast attacks, which by the time they are detected, have already produced disruptions or other damages. This delay can be avoided by using sensors that do their own packet captures and analysis, but in order to do this, the organization might have to purchase more powerful and/or more sensors.

NBA systems are often integrated with other security or network management tools, such as intrusion detection or intrusion prevention systems, in order to offer a 'complete' security solution. Depending on the type, the NBA sensor can have different intrusion prevention capabilities. For example, an inline sensor can perform inline firewalling. Most NBA sensors allow the administrators to specify the prevention configuration for each type of alert, but usually the prevention capabilities are limited (or not at all) in order to prevent the possible problems which can arise from false positives.

Present situation and trends. Currently there are many vendors offering network behavior analysis solutions, among which we can list Mazu Networks, Lancope, Arbor Networks etc. There are also big players like Cisco, whose MARS system (Monitoring Analysis and Report System) includes NBA functions or Nokia with its intrusion prevention system which incorporates IDS/IPS functions, vulnerability analysis and network behavior analysis. The trend is to deploy such systems in the organizations: according to Gartner, by the end of 2007, approx 25% of companies will implement tools for monitoring traffic for potential breaches. Currently there is no fully open source NBA product, but starting with November, this year AKMA Labs will offer its FlowMatrix software product for free to institutions, non-profit organizations and personal use. FlowMatrix is a software-only NBA system, running on Windows Servers and using traffic

data captured in NetFlow format. The initial learning period is approx 7 days, and the response time around 1 minute. In order to lower false positives, FlowMatrix uses multidimensional behavioral models. The system also offers the administrators the possibility to create manual rules.

In addition to security, recent approaches propose network behavior analysis also for network performance and optimization. The idea behind is that in order to optimize the IT infrastructure and its network, an organization requires visibility into the current and historical user behavior as well as applications and infrastructure configurations. Network Behavior Analysis can help the organization not only look to the past or present situation, but also to anticipate the impact of new applications and how they will affect the infrastructure and service levels. This trend was adopted by some major players in the NBA area, such as Lancope and Mazu Network, and their current products reflect it and they are advertised not only as security tools, but also as network profiling and optimization tools.

The reason, apart from their use it for network optimization, can be that this is also a good opportunity to expand their addressable market. For example, a research conducted by Yankee Group shows that the market for pure-NBA tools is estimated at approx. 125 million US dollars, while the market for network performance management software is approx. 1.3 billion US dollars (from which the passive monitoring tools that capture flow data to analyze performance comprise 500 million US dollars).

Conclusion

As we saw, the network behavior analysis is a technology which doesn't replace, but complements other security technologies like firewalls, intrusion detection/prevention etc. And even more, it can be useful in other areas such as network optimization. The NBA market is growing every year, and an increasing number of organizations start to adopt this technology as a standard, given its benefits. The technology is mature, but of course there is always room for improvement and the future will prove it.

References

1. Karen Scarfone, Peter Mell, *NIST 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)*, Feb 2007

2. George Hamilton, *Adjust Your Behavior: Network Management Incorporates Behavioral Analysis to Optimize Performance*, Yankee Group, Aug 2007

3. Denise Dubie, *The business of network behavior analysis*, Network World, Sep 2006, http://www.networkworld.com/news/2006/100206-specialfocus.html

4. *Nokia Intrusion Prevention offers advanced protection for the "dissolving" network perimeter*, Press Release, 15 nov 2006, http://www.nokia.com/A4136001?newsid=1088521

5. *FlowMatrix*, http://www.akmalabs.com/flowmatrix.php