GIAC CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

What’s in an Integrated Security Device?

Benjamin Llewellyn
GSEC Version 1.4b, Option 1
27 January, 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

"Small-to-medium sized offices often do not have the resources and dedicated IT personnel needed to manage multiple, complex network security products"

-- Gail Hamilton, executive vice president, Symantec Corp.[1]

Introduction

With every passing year our data networks become more essential to business. As they become more important, they also become a target for attacks. Network and data security takes higher and higher priority. As networks became more complex, more openings and opportunities for malicious exploitation develop. In turn, multiple types of security tools were implemented at various levels – virus scanners, firewalls, access control lists, system policy enforcement, and the like.

However, malicious threats have quickly become more advanced, and attacks have begun to utilize exploits at multiple levels in conjunction for maximum effectiveness. The detection of these attacks requires correlation of data from many security layers. The hours of labor required completing these tasks increases exponentially with each new security device. The cost of security increases as quickly, and it becomes economically infeasible to execute without some sort of automation. Integrated security devices can help solve these problems, and are an important part of modern security.

Business Need

Security functions at various levels have been automated to a fairly good degree. Devices and tools such as firewalls, virus scanners, authentication, auditing, and so on are widely implemented. These tools help make security more efficient at different layers of defense, but the problem of inefficient scaling of multiple layers of data security remains. It is still costly to implement and manage the security at all these separate levels, and to correlate the data quickly into meaningful conclusions.

Organizations have a business need to streamline the task of network and data security. This need drives the development of the new class of security device. The goal is to reduce the labor burden of security integration and management task, especially the automation of more complex and high-level tasks, such as data correlation.

The need for effective security exists and cannot be compromised. With complex security requirements, we need tools to:

- Reduce device implementation complexity
- Reduce device management complexity

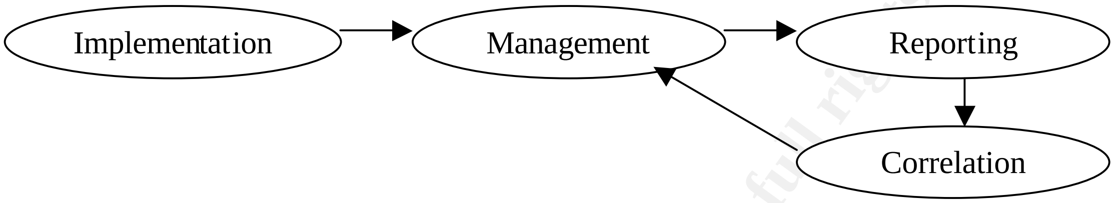
[1] Symantec Corporation. "Symantec Ships First-of-Its-Kind Integrated Gateway Security Appliance."

© SANS Institute 2003, Author retains full rights.

- Reduce device reporting complexity
- Reduce device data correlation complexity

These are related as shown in Figure 1.

Figure 1. Management lifecycle



Device Implementation

In project management, an important reason to ensure quality at early phases of a project is the general rule: cost of rework increases exponentially over time. This is true for many applications, security devices among them.

Integrated security devices can be very complicated to install and configure. It is very important to be able to fully install and configure a security device correctly the first time. A mis-configured system in the device can become very costly later on in terms of reconfiguration time, and the cost of a possible security compromise could be enormous.

Some features that make this a better process include setup wizards and automatic setup through network detection (of IP and network addresses, protocols implemented, and so on).

Device Management

Reducing the complexity of managing the device is the point of implementing an integrated security appliance in the first place. There is no need for an integrated box of different security devices if they are not managed in an efficient way as well. This is the core process of the device lifecycle.

How easy, feasible, and foolproof is it to manage and re-configure the device? Useful LEDs, system alerts (relating to device functionality, separate from security alerts), graphical management interfaces, and management interface portability can all work to make device management a more efficient process. These are the front-end cornerstones of effective device management.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Device Reporting

The problem here is the multiple formats of output from various security devices, and the ability to easily retrieve information about a single incident from multiple security devices. It is a common problem that incidents may pass unnoticed, or they may be very difficult to analyze without complete information. Complete information includes data about the incident from multiple devices.

Whether by a proprietary method, or by a standard such as the Intrusion Detection Message Exchange Protocol (IDMEP), some form of common scheme for describing device logs and results is necessary for external devices and administrators to understand the data.

Data Correlation

The purpose of a common data reporting and logging scheme is to be able to analyze the disparate data and to draw a meaningful conclusion that can be acted upon. This can be aided by making related data easy and fast to access across different devices (augmenting human correlation) and rule-based analysis.

An ideal method of analysis for an administrator would be if the system used rules to pick out interesting traffic, and for the administrator to see all the information relating to that traffic, including possible packet dumps, rules that were fired, other packets in the flow, traffic from the same address that were blocked by the firewall, and possible outbound traffic to the same host. This data comes from many different sources, and it would be a boon to an administrator to be able to look at any aspect of the incident quickly and comprehensively.

The last step in the general administration process would be to change existing rules (such as on a firewall device) to reflect what was learned in the correlation step; this cycles back to device management.

Features

Integrated Security Appliances are a relatively new device category. New combinations of security tools are being tested and released. However, most integrated devices share certain features:

- Firewall capability
- Automated Setup
- Integrated Management

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Firewalls are very basic security devices, and straightforward to implement. It is a cornerstone to implement and enforce advanced policies that are constructed by other tools, such as IDS, correlation engines, and administrator rules.

The automated setup and configuration of the integrated security device attempts to meet the business requirement of streamlined security processes. Modern setup wizards and auto-sensing of network parameters aids this goal. This is also one of the key focuses of an "appliance" device, and follows the Plug-and-Play ideal.

The business goals of reduced costs over time is achieved by the integrated management and configuration tools that attempt to successfully extract and correlate security data, either by simply displaying them in an easily-navigable fashion, or by using a correlation engine to derive conclusions (rule- or anomaly-based) from the data. Integrated security devices almost universally feature some sort of integrated management interface.

Other components that are found in many integrated security devices include:

- Intrusion Detection System (IDS)
- VPN functionality
- Content filtering
- Virus scanning
- Application level security exploits (URL manipulation)
- Alert, logging, and reporting interface
- Dynamic configuration mechanism

IDS functionality is a popular choice to include in a security device because of its versatility and power. It includes functionality to analyze traffic based on rules by packet, or anomalies in the protocol, and send various alerts depending on the rules. The IDS functions as the correlation engine, the thinking part behind the firewall.

Many devices designed for the edge of a network also include VPN functionality. As VPNs are used as a secure means of communications by remote locations via the Internet, VPN support typically falls under the same management area as other security devices. It is a popular value-added feature to an integrated security device, and integrating it with the other functions in the device makes it easier to consolidate log and report data for administrators.

Content filtering is a more performance-costly, but valuable function available in some integrated devices. It takes quite a good deal of extra hardware time and resources to analyze the upper layers of a packet, as opposed to lower-level protocols. Some implementations, however, have designed this function to operate concurrently with the IDS analysis of a packet. This requires duplicate hardware, but greatly reduces the performance cost of this feature.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Virus scanning is closely related to content filtering, and is usually implemented within the scope of content filtering. However, when virus content is detected, there are rule options that are exclusive to this process, such as attempting to clean an infected file. It is also somewhat more resource intensive than the usual content filtering, having to support logical analysis of content, instead of simpler pattern matching.

Still within the scope of content filtering is Application-level security. Content filtering is essentially a static process that reflects company policy. Virus scanning looks for malicious code signatures that would indicate a virus. Application-level security attempts to identify application-level exploits. A good example of this is mal-formed URLs that result in unauthorized directory traversal. Although the URL may be technically legal, it exploits weaknesses in the system and causes a security breach. Applications and the security risks associated with them are many and varied, and it takes a strong analysis engine, and rigorous updating to be effective. At the same time however, this process also utilizes a large amount of resources.

The alert, logging, and reporting interface is an extension of the management toolset. While the management tools will include these basic features, some devices come with the flexibility for many different methods of alerting, logging, and reporting. Some examples of this include alerting by pager, via SNMP, logging traffic in binary, compressed, to a database, to an SMS log server, with partial or complete packet dumps, and reporting using analysis tools, Crystal Reports, database query suites, and so on.

The last major feature is the dynamic configuration capability. This could also be a potentially dangerous feature. It is a basically a rule set defining what changes to make in the security policy and settings (such as on a firewall) based on the results of correlation. In other words, automated configuration changes without human intervention. There are certain situations where this is very beneficial; such as when an outbound response is detected that contains sensitive data. A rapid termination of that communication could be very important. However, it is also important that this type of function cannot be exploited by malicious attackers to initiate a self-caused Denial of Service attack. An example would be a dynamic configuration rule that says to block an IP that is sending a DoS flood, and a hacker who spoofs a business partner's IP address.

The way that the integrated tool performs displays data plays a major role in the overall benefit of the device. Without effective display of the data, the integrated device is simply a number of separate security devices in one box with no real benefit. Small-scale dynamic configuration can be very effective in reducing cost. These “meta”-rules, or rules describing when and how to change existing rules, can save large amounts time for technical staff.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Downside

There are issues with the use of an integrated security device. These primarily have to do with the (in-) flexibility involved when dealing with a proprietary vendor. The first concern has to do with, "How many options come with the device?" Basically, what sort of protocols and interfaces are supported. This is related to questions like: What options are available for data output? Is it necessary to purchase middleware to export the logs to a database? Are the logs stored in a proprietary format, or in simple TcpDump binary?

If the organization has a requirement for a certain logging or reporting method, and the device does not support it, then it becomes unusable. Middleware could be developed separately, but that requires extra time and overhead, and the robustness of the middleware would have to be carefully monitored, leading to extra costs.

A major concern is the flexibility of allowing custom rules, and to modify or delete default ones. Must rule updates come from the vendor? How quickly does the vendor respond to new threats? Rules from vendors are not infallible; can they be modified or uninstalled if they are written incorrectly, or if they hinder the network? Would that violate any support agreement or warranty? Firewalls have simple and straightforward rules … but what about IDS rules? Can data correlation rules be tweaked?

The utility of an integrated security device can very limited without the ability to tailor the detailed configuration to the needs of the particular network. Typically, the more an integrated device becomes an appliance, the less flexible the configuration options become. Many attacks are simply irrelevant to a specific network, depending on what is running. Rules that fire on these irrelevant attacks are false positives and can be very counter-productive to the business goal in implementing the device: to reduce administrative burden.

Another issue that must be considered is performance. An integrated security device may perform several functions on a stream of data. From simple firewall-style access lists, to stateful packet analysis, content filtering and a host of other functions, the device could easily introduce a major latency issue on the network. This is also where the ability to configure rules comes into play in a very significant way. The default rule set that comes with the device often includes many rules that are superfluous to the particular network, and can waste a large amount of hardware resources. Unnecessary rules also add to the complexity of analysis and forensics actions.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Examples

There are a number of integrated security products on the market. Here are a few examples that show devices that focus in different areas (function vs. performance).

Symantec Gateway Security

This appliance is an edge-device. It includes the standard firewall and integrated management tools. It also has anti-virus, Internet content filtering, intrusion detection, and VPN functions. It comes with automatic virus and IDS signature updates, an installation wizard process, and a common management console. It is advertised as a "plug-and-protect" device. (Symantec)

Celestix

Their Celestix one FV line of appliances features Firewall and VPN functionality. They also have high availability software that ensures 24x7 service. It is a focused appliance, and advertises fast throughput for VPN traffic. It also features a web-based management interface. (Celestix)

SonicWALL

The SonicWALL GX appliances are advertised as high-performance and high-availability Firewall / VPN devices. They also include IP address management and a web-based management and reporting tool. It also supports direct integration of anti-virus and content filtering. (SonicWALL)

Resilience

The Resilience DX4000 is an integrated Firewall / VPN device. It has built-in physical redundancy and a modular design. It also features a fast setup process, and CheckPoint management tools. It is a geared towards performance and availability. (Resilience)

Fortinet

Fortinet's FortiGate family of products includes a wide array of features, including firewall, virus scanning, content filtering, VPN, and intrusion detection functionality. It also includes a web-based management console. It uses ASIC technology to improve performance of the more hardware-intensive tasks, such as VPN encryption. (FortiNet)

Secure Commerce Systems

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The GuardTower Security Correlation Appliance is a back-end device that integrates with regular security devices such as Firewalls, IDS, and so on. It advertises incident response features, in addition to detection and analysis. This device fills in the intelligent correlation process in Figure 1. It functions at the same area where a great deal of administrative effort takes place – the extraction of data from multiple sources and correlation of that data to formulate a response. (Secure Commerce Systems)

As is described, products such as Symantec's and Fortinet's are feature-rich. While they can have good performance, they won't be able to reach the level of throughput of Cenestix, SonicWALL, or Resilience. These feature-focused products (Firewall/VPN) are built with the core network in mind. They are intended to add functionality to a system area that requires high performance. The feature-rich products start with providing many functions, and try to optimize performance (and lower administrative complexity and overhead). These are aimed towards smaller networks (an all-in-one solution), and simplify a system area that requires complex features.

And last, Secure Commerce Systems' attacks the problem from a different angle – as a device that functions "out-of-band" so to speak, performance is not as much of an issue, and the full force of analysis features is applied to the data result from regular security devices. The deficiency in the approach, however, is that real-time response is hindered by the delay of the data being transferred to the GuardTower analysis system.

Conclusion

There are a variety of new devices in the marketplace today that integrate many security functions into one box. They can save time and headache for administrators with simplified installation. Device maintenance is simplified with unified management tools. Troubleshooting and analysis is also made more efficient. Time savings equates to cost savings, and this is good for business.

At the same time however, integrated security devices can be too "user-friendly" and not allow sufficient tweaking and modification to be effective. This can lead to costly performance degradation and management overhead. Automated reconfiguration rules that are too aggressive can be exploited by attackers.

Although the devices on the marketplace today include more functionality and performance as time goes on, they are focused in specific network areas, such as at the core or edge of the networks.

Integrated security devices have their ups and downs. Properly designed and implemented, they are very valuable tools in security.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Celestix Networks, Inc. “Features-FV930 Security Appliance.” URL: http://www.celestix.com/products/FV930/features.htm (30 Dec. 2002).

FortiNet, Inc. “FortiGate 500.” URL: http://www.fortinet.com/doc/FortiGate500.pdf (30 Dec. 2002).

Huston, Brent. “The Age of Security Appliance.” 22 August 2001. URL: http://www.itworld.com/nl/security_strat/08222001/ (30 Dec. 2002).

Resilience Corporation. “Resilience: Solutions & Products.” URL: http://www.resilience.com/solutions/dx4000/dx4000_features.html (30 Dec. 2002).

Roberts, Paul. “INFOSECURITY : Appliances of every flavor for 2003.” 13 Dec. 2002. URL: http://www.itworld.com/Sec/2210/021213securityapps/ (30 Dec. 2002).

Secure Commerce Systems. “Secure Commerce Systems eCommerce Security Solutions.” URL: http://www.securecommercesystems.com/guardtower.html (30 Dec. 2002).

SonicWALL, Inc. “SonicWALL - GX250/GX260.” URL: http://www.sonicwall.com/products/gx250.html (30 Dec. 2002).

Symantec Corporation. “Symantec Enterprise Solutions.” URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=133&EID=0 (30 Dec. 2002).

Symantec Corporation. “Symantec Ships First-of-Its-Kind Integrated Gateway Security Appliance.” 16 April 2002. URL: http://www.symantec.com/press/2002/n020416.html (30 Dec. 2002).

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.