

# *Information Security: A Defensive Battle*

Avi Chesla

**M**edium to large networks usually comprise different types of security components. To establish an efficient security architecture, an engineer must fully understand the major role of each security component, its comparative advantage, and natural position. Although this article does not mention every type of the existing and emerging security product, it is possible to apply the battlefield analogies to virtually every type of security solution to simplify the complicated architecture of today's data networks. The basic security platform comprises a layered approach and an efficient way to synchronize security products at different layers of the network.

In many ways, information security may be thought of as a defensive battle. Conjure up images of uniformed fighting troops, clever intelligence specialists, and hardcore decisive leaders. In time of battle, these elements come together to become a fighting force. Leaders at all levels, from squad leaders to corps commanders, synchronize and control the troops on the battlefield. They do this based on the picture of war that they construct from pieces of information collected before and during the battle.

In the realm of information security, *actions* such as resetting connections, filtering packets, sending misleading information to attackers, and directing traffic to "honeypots" are all activities that can be associated with the actions of the fighting troops on a real battlefield.

Continuing this comparison between information security and warfare, *decisions*, such as when and if to initiate defensive actions, are the responsibility of decision engines embedded into security products and solutions. These mechanisms can be best compared with the combat leaders who are charged with correlation and analysis of information before and during the attacks. Like information security products, battlefield commanders must quickly come to conclusions and take some kind of action before the situation becomes catastrophic.

*Sensors*, which are normally installed both in today's data networks and on the physical battlefield, are responsible for providing the leaders (decision makers) with valuable information about the enemy and the environment. Here is yet another comparison applicable to information security

---

*AVI CHESLA currently serves as Director of Research for Vsecure Technologies (U.S.) Inc., a developer of innovative intrusion prevention products. He is a graduate of Physics and Mathematics from Tel Aviv University and has been focusing on next-generation security solutions since 2000. As is the case with the majority of the Israeli population, he also serves as a soldier in the Israeli Armed Forces reserve. His command of armored units directly contributes to his unique perceptions of information security and warfare. Avi can be contacted at [avic@v-secure.com](mailto:avic@v-secure.com).*

personnel and the intelligence specialists on the real battlefield.

As in any kind of battle, whether it is defeating hackers or overcoming an opposing fighting force, victory absolutely depends on the ability to coordinate all defensive resources in the most efficient way. Cooperation between forces is always a complicated task because every force is assigned to deal with a different type of problem. It is generally assumed that the nature and composition of each force is also different. Each force was specially built and trained to work in its own threat environment. Cooperation between security network components, just like military coordination during the “fog of war,” can be extremely complicated.

Several methods are being used to create cooperation between forces, including:

1. Every force needs to know what its physical and operational boundaries are and who sits within and beyond them. These boundaries help the force stay in focus and handle threats in the most efficient way based on their training. Using this principle, every force will deal with only the threats it was assigned to deal with, and will not waste its resources on assignments that it cannot handle or can only partially address.
2. Every force needs to be able to communicate with other forces. Common language or predesignated signs are something that every force needs to learn and know. Without an effective communications protocol, it will be easier for the attackers to bypass the defensive forces.
3. Every battle needs a leader. A capable leader is familiar with all the forces’ capabilities and weaknesses, and knows how to control and synchronize the forces in the most efficient way according to the present situation, which the leader also must know.

These methods are conceptually very similar to the methods that network security components need to follow to establish a consolidated and coordinated information

security defense that one can consider as a Basic Security Platform.

The *Basic Security Platform* is defined as the baseline defensive structure using existing security technologies and products to effectively protect a network in the most effective way. This platform will fully define a proposed strategy for defending the network by allowing each security component to stress its comparative advantage and work in cooperation with the others.

This technical, vendor-neutral article explains the author’s concept of the Basic Security Platform using the theme of defense in layers. It outlines the comparative advantage of each security component and places it in its most appropriate layer between the network’s natural boundaries. The article emphasizes the functionalities of perimeter security products in such a platform, and describes the relationship between perimeter components and the internal components in the platform. The thrust of this article is to explain why and when central management systems are crucial as part of effective information security efforts.

#### **DEFINING THE STRATEGY OF DEFENSE**

In a real battle, the strategy of where to initially position the fighting and intelligence forces needs to be followed by a plan that will carefully examine the possible anticipated attack scenarios. To prepare a real defensive plan, one first needs to pinpoint the critical or essential geographical areas that one cannot afford to lose. Then one needs to analyze the weak points of these essential areas. The basic assumption is that every essential area has its weak points, and the only way to be able to anticipate the ways that this area can be attacked is first to be aware of its weaknesses.

One must carefully analyze every possible attack scenario that can have an impact on critical areas before one actually positions one’s troops. Every attack scenario, from the most trivial and easy-to-perform to the most theoretical one, needs to be examined and taken into consideration. Tacticians will

*Cooperation between security network components, just like military coordination during the “fog of war,” can be extremely complicated.*

*Like a battlefield commander, an information security engineer should carefully learn his network's vulnerabilities, decide which areas or specific equipment are most vulnerable or critical, and then simulate "all" possible attack scenarios that might have a negative impact.*

acknowledge that these initial steps in defining the defensive battle are a crucial step. Without them, it will be impossible to successfully confront the attackers.

These specified initial procedures are very similar to the ones that need to be taken when establishing an information security platform. Like a battlefield commander, an information security engineer should carefully learn his network's vulnerabilities, decide which areas or specific equipment are most vulnerable or critical, and then simulate "all" possible attack scenarios that might have a negative impact. Only then should the engineer decide what type of security products are needed to mitigate damage and risk.

Continuing with the warfare analogy... after selecting the essential geographic areas, understanding their weakest points, and anticipating possible attack scenarios, the commander needs to choose the nature and composition of the troops that will be most suitable for protecting these areas' vulnerabilities. An urban area normally calls for short-range combat that can be done by forces properly trained for street warfare. Open areas will require troops that are trained to fight in that particular environment with powerful long-term resistance capabilities against long-range invasion attempts.

As in the case of warfare, after the information security engineer identifies the organization's critical network components, and understands their vulnerabilities and the possible anticipated attack scenarios, this engineer needs to move to the next stage and choose the most suitable security product that will be able to deal with the analyzed vulnerabilities. Conceptually, this procedure is very similar to the one used in real physical warfare.

The next section examines the nature of existing security products and provides an understanding of their comparative advantages to know how to best position them in the security platform.

### **DECIDING FORCE POSITION AND BOUNDARIES**

A defensive battle requires different kinds of forces that will be able to perform a variety of defensive operations. A successful defensive battle requires the ability to perform the following basic defensive operations:

- Short-range combat.* An urban area will require short-range combat that can be done by troops that are trained for street warfare. These troops are specially trained to be capable of recognizing and eliminating specific targets in a very efficient way, but may not be specialized in defending against open-area, large-scale attacks.
- Deception.* This operation involves techniques that will cause attackers to be diverted from attacking real essential areas, leading attackers to waste resources on false targets.
- Perimeter combat.* This kind of combat requires troops to fight in the open with powerful long-term resistance capabilities.
- Camouflage.* This consists of operations that mask the essential areas in a way that will prevent intelligence gathering that may expose weaknesses.
- Intelligence operation.* To "know the enemy," it is necessary to gather information before and during the battle. In addition to various methods such as sensors and spies to collect intelligence on the enemy, valuable information also

comes during actual defensive operations, in which an enemy can be directly observed and assessed.

- *Patrol troops.* These troops will be required to find infiltrators that may have already penetrated through all lines of defense.

### Layers of Security

A defense in layers approach is an inherent part of an effective information security program. As attacks against networks have increased and grown in sophistication in recent years, security product companies have developed a number of new information security technologies. This has further underscored the need for a well-thought-out implementation of a layered security approach. As new products were integrated into a network security program, their placement and “operational boundaries” were defined. For example, some products were found to be best placed at the network edge, others near critical servers and possibly in the DMZ. As in a real battle, these boundaries help the force remain focused and handle threats in the most efficient way based on the force’s skills.

**First Layer of Defense.** The first layer of defense includes security products designated to closely protect the internal network’s critical components. Some of these were also considered the network’s last line of defense. These products include host- and server-based intrusion detection and prevention systems, network-based intrusion detection sensors, personal firewalls, anti-virus software, application-specific security such as Web or e-mail protection products, file integrity checkers, and a few others. To work efficiently, these products must be deployed on the hosts they are supposed to protect, closely in front of or on a critical network segment — these are the product’s operational boundaries. In the metaphor to real warfare, these are the force’s operations boundaries. All of these products must have the capability to precisely diagnose the communication and the

protected system operations, decide if malicious activities are in progress, and be able to stop them as quickly as possible.

- *Host- and server-based intrusion detection systems.* These systems must be able to detect critical files being accessed, buffer overflows, rootkit installations, Trojan versions of system files, and exploitations of system vulnerabilities. The aim is to simply prevent these kinds of malicious activities. These products need to be able to detect certain incidents through precise behavioral analysis and perform such operations efficiently. For example, these security solutions must be able to determine that a code about to be executed by the operating system has originated from a normal application or from an overflowed buffer. The security product must also be able to detect a growing list of known attack signatures (through pattern recognition). Such operations require deployment on the host itself, meaning very tight boundaries of operation.
- *Application-specific security products.* These systems must be able to perform operations that focus on the application they are supposed to protect. A widely deployed example is Web server protection. These security products need to analyze cookies, HTTP requests and corresponding error replies, Web content, etc., in order to detect malicious interaction between users and the Web application. Interactions that do not conform to the rule set of allowable application interactions need to be blocked. High-resolution examination of the communication and system operations up to the application level requires that these products are deployed on the servers themselves, in front of them, or on a critical segment of servers to allow them to work properly. These are the products’ natural boundaries of operation.
- *Network signature-based intrusion detection and prevention systems.* These systems perform pattern recognition

*Some products were found to be best placed at the network edge, others near critical servers and possibly in the DMZ.*

*Perimeter security products follow very similar characteristics that can be associated with the perimeter forces in a real defensive battle.*

operations. These systems need to be deployed in the network's critical segments to detect predefined attack signatures. To enable these types of products to be able to perform their job properly and without excessive amounts of false positives and misdetections, they must be updated with the most recent attack signatures and be aware of the network component types they are supposed to protect (i.e., operating system versions, server applications, TCP/IP stacks, etc.).

- *"Honeypot" and "honeynet."* Another type of product that can be associated with the first layer of defense is the "honeypot." Such products try to deceive the attackers and divert them to virtual or special servers that are not the real production servers of the protected organization. In doing so, the "honeypot" product causes the attackers to perform their malicious operations in an isolated environment (i.e., a ghost server or a whole ghost network — "honeynet") without causing any real damage to the real production organization's servers and hosts. This kind of protection also makes a significant contribution to the investigation process of new attack trends and exploits. Now, to the warfare analogy. These "honeypot" products can be associated with special forces that are responsible for deceiving the enemy by using, for example, fake targets. Additionally, these products can also be associated with real intelligence forces, forces that are responsible for investigating and learning the method of attacks the enemy is planning to use in the future.

The characteristics of all the aforementioned products belong to the first layer of defense, just as certain field forces are the first line of defense in combat. Short-range combat troops are trained to deal with street warfare, that is, recognizing threats in very high resolution, and capable of quick

response and removing the threat with surgical precision. All of these, including operational boundaries, are characteristics similar to those required from first-layer products. The absence of first-layer security products between these boundaries would lay to waste most of their comparative advantages and result in insufficient protection.

### **Second Layer of Defense: Perimeter Security**

The second layer of defense includes security products that need to deal with attacks that are defined as perimeter network attacks. Products such as perimeter network security products, firewalls, routers with integrated security functionalities, and a few similar product categories can all be considered part of the second layer of defense.

The main capabilities of firewalls and routers are network access control and VPN (virtual private network) functions. They are generally deployed at the gateway of the organization or on internal network segment junctions.

### **Perimeter Network Security Products.**

These products are relatively new to the information security market. They were designed to confront network vulnerabilities for which the first layer and other second-layer products were not designed to deal.

Perimeter security products follow very similar characteristics that can be associated with the perimeter forces in a real defensive battle. Perimeter forces include the fighting troops that were trained to be able to push out large-scale and massive attacks. The fighting force must be escorted by the perimeter intelligence troops that are trained to collect strategic long-term and tactical short-term intelligence information. It is the nature of all perimeter forces to be able to

construct a wide picture and perception of the enemy. Perimeter forces can recognize large movements and trends of the enemy by stationing themselves in key areas throughout the battlefield. Through this method, they can detect unusual dynamics that can ultimately become a threat to the force.

Perimeter forces are not necessarily trained to be able to detect in very high-resolution the behavior pattern of the individual (i.e., the ability to detect a “wanted” picture). This is the job of the close-combat forces. Instead, the perimeter forces are trained and assigned to detect unusual and offensive movements over the border in the enemy territory. On the one hand, the perimeter forces cannot hermetically stop all threats, meaning that some infiltrators will be able to penetrate the areas in which the perimeter forces are positioned. These intrusions will be detected and stopped by the close-combat forces. On the other hand, the close-combat forces will never be able to see and construct a wide picture of the enemy’s movements and analyze them as the perimeter forces can do. Additionally, and most importantly, these close-combat forces may collapse or will suffer from a reduction in their functionalities, meaning an inability to perform what they were trained for; this is especially the case if the perimeter forces are unable to repel large-scale and other attacks that should be easily defeated by forces in the perimeter areas.

Because of resource limitations, it is a fact that close-combat troops cannot be everywhere, especially when large areas must be covered. To overcome this, close-combat forces need to work in cooperation with the perimeter forces, which have more coverage capabilities. This issue is discussed in the next section, which focuses on the synergy between the layers of defense.

In the realm of information security, second-layer perimeter security products will stress their comparative advantage if positioned on the network’s border facing the external world. This external world is the Internet. These borders are the operational

boundaries referred to in the warfare analogy. Perimeter information security products must be able to construct a complete picture of communication characteristics going into and out of the protected network in order to establish normal baselines that best suit the protected network. They must have the ability to detect deviations from these lines, decide about the threat these deviations can impose on the protected network, and then filter or block them accordingly. These kinds of deviations usually reflect the ongoing distributed denial-of-service (DDoS) flood attacks. Perimeter security products must also be able to detect pre-attack probe activities that include various kinds of network scanning techniques. Because these activities’ objectives are to probe every possible network component to construct a picture of the protected network’s topology, they can only be detected through an analysis conducted from the border gateways. That is, the detection and prevention of these activities is also the responsibility of the perimeter security products.

Worms, which can automatically propagate through the network’s borders into the internal components, are also the responsibility of the perimeter products to detect and prevent. Worm alerts can be initiated as a result of the following two occurrences:

1. Worms usually cause a deviation from the normal adapted traffic characterization as they significantly change the amount of traffic they cause during the propagation process.
2. Worms usually perform network scanning activities to discover potential hosts they can exploit.

Network perimeter security products are normally used to detect this type of malicious activity.

Perimeter security products must also be able to perform masking operations such as network address translation (NAT), which is designed to hide the internal network component’s addresses and reduce the probability of being attacked from the outside (similar to the

*Perimeter security products must be able to detect pre-attack probe activities that include various kinds of network scanning techniques.*

*A SIM system provides a mechanism to use a common language between all security devices in the network — if all of the products are capable of supporting common protocols and can send data to a central management application or console.*

camouflage operation in a real battle). Perimeter firewalls and routers, in addition to access control and VPN functionalities, are usually responsible for NAT operations.

All of the above incidents will be handled in an efficient way by the second layer of defense products. If these incidents are not handled in the perimeter area between the second layer's boundaries, one would see inefficient functionality of these perimeter products.

Another important responsibility of second-layer products is to protect the internal security components (first-layer products). Without the effective functioning of second-layer products — meaning the inability to efficiently filter the attacks they were supposed to deal with — the first-layer products would suffer from a decrease in their functionalities, a vulnerability to denial-of-service flood attacks and, as a result, the whole network will be more vulnerable to all kinds of attacks.

#### **Breaking the Layer's Boundaries**

During the past two years, a few vendors have tried to unite different kinds of security functionalities and put them in the same box — often called an all-in-one solution. This approach sometimes tries to put different layer products in the same box, and usually results in a degeneration of each one of the security functionalities it includes. Although small organizations can benefit from such an approach (mainly for cost-benefit reasons), it is not recommended that medium- to large-sized networks do this because of the efficiency reasons mentioned above. Another consideration that weighs against an “all-in-one” approach is that it presents a potential single-point-of-failure issue.

#### **THE SYNERGY BETWEEN FORCES**

In battle, each force must be able to communicate with other forces. This relies on a

common language or predesignated signs that every element of the force needs to learn and know. Without effective communication protocols, it will be easier for the attackers to bypass the defensive forces. Again, this concept directly applies to network information security.

Although correct positioning of security components in the protected network is important, it is not enough. The security engineer must verify that the security components are able to communicate with other products, such as central security management systems, network management systems, and other security components. This is an important part of the complete establishment of the security platform. Cross-communication will improve the functionality of each individual security product and result in an entire network that is less vulnerable to attacks.

It is very important to have the ability to control and manage all of these different types of products through a single device when dealing with medium to large networks that usually include products from multiple vendors. Security information management (SIM) products are designed to monitor, correlate, and control the various elements in a multi-vendor security environment. A SIM system provides a mechanism to use a common language between all security devices in the network — if all of the products are capable of supporting common protocols and can send data to a central management application or console. The task of the central management system is to aggregate, correlate, and analyze the security information that is collected from the different security devices in the network. The result is a more robust decision regarding attack detection and more accurate estimates of the level of the threat each incident presents. Central management also helps reduce the excessive

amount of unnecessary security alerts and improve the quality of forensics information that can result with the discovery of new attack tools, exploits, worms, Trojans, etc.

We use the following example to underscore the necessity of communications between multiple products from both security layers through a central security management system.

In this instance, a perimeter security network product, which is part of the second layer of defense, detects network-scanning activities that are trying to locate the existence of SQL servers in the network.

### Scanning Activities

Scanning activities are very common phenomena, especially against large-scale networks. The number of scanning attempts against large networks can easily reach several hundred incidents per day. Many of these activities are initiated by automated tools that randomly scan the Internet and have a negligible influence on the networks, meaning very low impact. However, these activities can also be followed by dangerous activities such as worm penetration, exploiting the application's known and unknown vulnerabilities, Trojan installation, installation of distributed denial-of-service agents on the protected network hosts, etc.

Cooperation between the different layers of defense should be established to determine more precisely the actual threat of these activities. If scanning activities that try to find SQL servers have been detected, this information should be collected by the SIM system. The SIM system also collects security logs from a host-based intrusion detection system that sits on the same scanned SQL servers in the network. The security logs that the IDS initiates can include information such as identification that a known exploit has been seen or that a system's file has been changed. Correlation of these security incidents by the central security management system results in more robust conclusions about the detected incident as all elements are reporting different but

complementary information to complete the overall picture.

The correlation between these incidents can result in the following:

- If a known SQL exploit is seen by the host-based IDS during or after the scanning activities alert, then this incident's level of threat will be raised to a level where the security engineer must be aware of it immediately and respond accordingly (i.e., block the source IP address that initiated such scanning activities by the perimeter security product).
- If no known exploits are seen but an attempt to modify system files are detected, then the level of threat should be raised and the incident should be further investigated.
- If no suspicious activities are seen by the IDS, then the level of threat should be low.

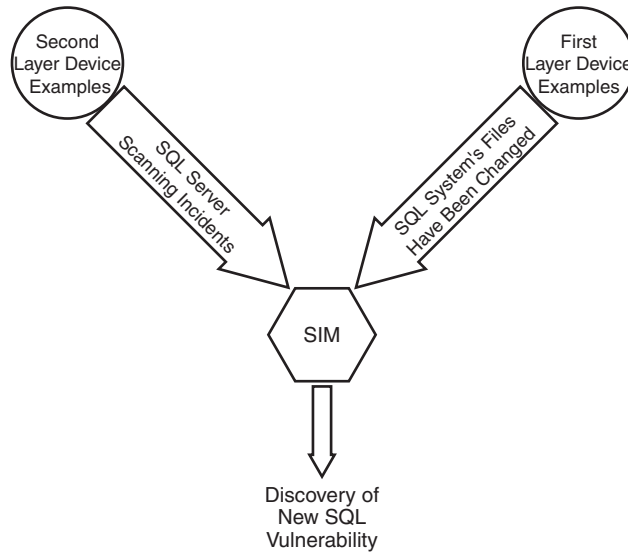
Figure 1 outlines a process in which an unknown vulnerability of an SQL server can be discovered.

### THE LEADERS

Real battle requires leaders at all levels — from squad leaders to corps commanders — to synchronize and control the troops on the battlefield. They do this based on the picture of war that they construct from pieces of information collected before and during the battle. Squad leaders can be associated with the decision engine supported by every information security component. These engines are directly responsible for the actions each component will take. Each component needs to have an efficient decision engine that will have the ability to quickly collect, analyze, and correlate the information the device supplies. It is natural that every device will use a different technology in order to support such engines according to the nature of attacks for which it was designed to deal. A decision engine can be very simple, as in the cases of access control devices, or more “intelligent” ones, such as in the case of active perimeter security devices, applications-specific protection devices, etc. It will be natural to expect

*Real battle requires leaders at all levels — from squad leaders to corps commanders — to synchronize and control the troops on the battlefield.*

**FIGURE 1** Discovering an Unknown Vulnerability of SQL



SIM: Security Information Management refers to the central security management system.

that the simple engines will come to conclusions quicker than the engines of the more “intelligent” devices.

Security information management systems — SIM products — can be compared to the corps commanders or generals in a real battle. These generals are an essential factor in large-scale battles. Like senior commanders who receive information from all levels of the fighting force, the management system must be able to analyze diverse information and make decisions impacting the entire network. This highly complex task requires sophisticated technologies, which are being introduced and improved almost on a daily basis.

## CONCLUSION

Medium to large networks usually comprise different types of security components. To establish an efficient security architecture, an engineer must fully understand the major role of each security component, its comparative advantage and natural position. Although this article did not mention every type of the existing and emerging security product, it is possible to apply the battlefield analogies to virtually every type of security solution to simplify the complicated architecture of today’s data networks. The Basic Security Platform comprises a layered approach and an efficient way to synchronize security products at different layers of the network. ■