Security in Depth

Over the past 25 years, the methodology of network security has changed almost beyond recognition. With the aggressive pace at which data have grown and the need for constant real-time access becoming the norm, paying increased attention to securing networks and data has become critical. As data become ever more available online and organizations are obliged to offer access to their information across a publicly mistrusted medium, the potential for and reality of data compromise have become very real. Organizations lose billions of dollars each year through this very phenomenon.

Security breaches seem to be a daily occurrence, one of the most recent being the Equifax breach, in which tens of millions of records were stolen. Although, at the time of writing, the actual cost of this breach remains unknown, it could easily approach the US billion-dollar mark. With this level of loss becoming a real risk, businesses are committing increasing amounts of resources to bolstering their data security. Such efforts have seen the movement to a layered defense model becoming the norm. Experts in the field are designing security measures so that information entering and leaving an organization must pass through several layers, in an effort to fill the gaps left by using a single security device. Some of these methods will be discussed in detail in this article.

Layered security is part of a larger strategy known as "defense in depth." Although these terms are sometimes used interchangeably, they are not the same. Defense in depth, which was developed by the US military as a policy and method of defense, is best described as: "A defense in depth approach to security widens the scope of your attention to security and encourages flexible policy that responds well to new conditions, helping ensure you are not blindsided by unexpected threats."[1]

Malware Defense

The prevention of malware is a significant factor when designing network security. How can one prevent malware from infiltrating the network? This pernicious software can be introduced in many ways. As an example, an email with a link prompting a user to download malware may be received; a user may mistype a web address and land on a rogue website designed to deliver malware; or a user may insert a malware-infected Universal Serial Bus (USB) stick into their computer. Once introduced, malware such as worm viruses can spread extremely rapidly to other unprotected, vulnerable computers and servers in the network.

With so many ways in which malware can enter a network, a single layer of protection is no longer sufficient. A popular method of layering defense against malware is to ensure that all data are scanned at least twice when entering and leaving the network.

To add another layer of protection, the scanning devices should be obtained from multiple vendors when possible. Malware protection typically works on signatures; using different vendors, with different signature databases, will fill in the gaps between signature update times to help protect against zero-day malware outbreaks. Security designers usually accomplish this goal by using malware protection end-point solutions for end-point scanning and layering these with email-scanning solutions and deep-packet malware scanning with a border device such as a firewall. This produces a multilayered scanning scenario. If someone sends an email to a user, the email is scanned for malware by the email scanner, then scanned again at the firewall level and then a third time by the end-point security software (**figure 1**). According to the US Federal Communications Commission, "The idea of layering security is simple: You cannot and should not rely on just one security mechanism to protect something sensitive. If that security mechanism fails, you have nothing left to protect you."[2]

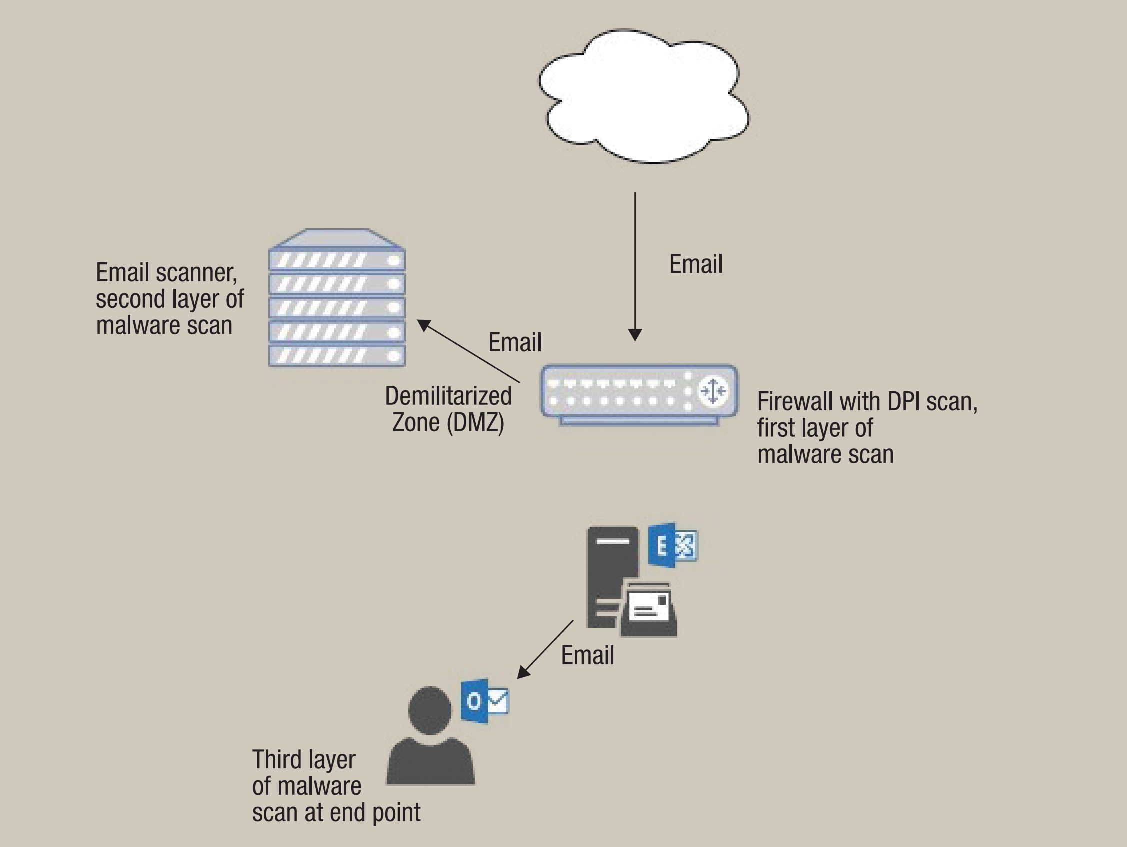
Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2GTPoh8

Charles Hale, CCNA, CISSP, MCSE
Is the chief information officer for Legacy Healthcare, a US healthcare company. He has worked in information technology security for 15 years. Prior to working in the healthcare space, he provided security consulting to a broad spectrum of biotechnology companies ranging from small start-ups to publicly traded companies. Hale has a passion for technology and data security. He has committed his career to protecting sensitive data for data owners.

Figure 1—Layered Malware Scanning


Email
Email scanner, second layer of malware scan
Email
Demilitarized Zone (DMZ)
Firewall with DPI scan, first layer of malware scan
Email
Third layer of malware scan at end point

Border Protection

The network security perimeter is the first layer of defense in any network security design.[3] Network traffic flows in and out of an organization's network on a second-by-second basis. The data move from an untrusted to a trusted network and *vice versa*, which is a huge concern to security designers. How can this "border" between the two areas be protected to ensure the trusted network remains secure?

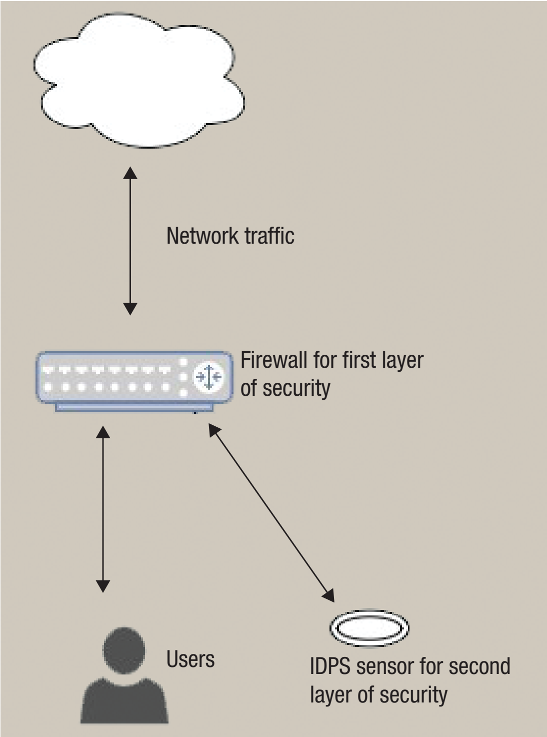
> “RESTRICTING SECURITY TO THE IMPLEMENTATION OF A FIREWALL ALONE IS LIKE LOCKING THE DOORS TO A HOUSE WITH NO ALARM SYSTEM.”

It was once held that the implementation of a firewall at the border and the network would be enough. That methodology is no longer sufficient in today's environment, where the untrusted network (the Internet) is a playground for hackers that is open 24/7. Restricting security to the implementation of a firewall alone is like locking the doors to a house with no alarm system.

Organizations need layered defenses at their borders, and the most effective way of obtaining that is through the use of both a firewall and an intrusion detection and prevention system (IDPS), preferably from different vendors so as to cover any vulnerabilities in the protection engendered by relying on a single vendor; any suspicious activity can then be reported (**figure 2**).

Firewalls may be extremely effective, but they cannot be relied on as the sole means of securing a network perimeter. In fact, the SANS Institute has determined this to be one of the seven most common mistakes made by management that jeopardize network security.[4] Protecting the border, although a high priority, is not sufficient. Security needs to evolve from protecting the edge of the network from unauthorized access and malware into a layered security approach.

Figure 2—Layer With Firewall and IDPS


Network traffic
Firewall for first layer of security
Users
IDPS sensor for second layer of security

Network Design

One of the most effective ways of achieving the goal of layered defense is through the design of the network. A flat network is the most vulnerable of all; networks with one single segment are vulnerable because publicly accessible resources must be accessed directly inside the network via the untrusted network (the Internet). For example, if an email server is positioned inside the network and accessed directly from the Internet and provides only one set of firewall rules, the security lacks any layers and is, therefore, weak.

How is the layered security model applied to offset this weakness? In short, security designers implement a separate segment between the two networks called a demilitarized zone (DMZ). This requires traffic coming from the Internet, and bound for the email server, to pass through the DMZ area first. Then, once authorized, the request for email access passes from the DMZ back through another, more restrictive, set of firewall rules to the actual email database. This allows the security administrator to be much more restrictive in terms of access. Without the DMZ, all network traffic bound for the email server passes. In contrast, with the DMZ in place, the administrator restricts traffic only from the web server front end to the email database in the trusted network, thereby accomplishing the goal of layered security via network design. An IDPS will also scan the network traffic, creating yet another layer of security.

In addition to adding a DMZ segment at the network entry point, additional steps can be taken to section off high-priority assets on the network. For example, in the banking industry, typically at least one segment is used that possesses the highest level of security in the internal network. In industries with extremely high-risk assets, protecting the data from the outside is extremely important, as is protecting them from the inside. When customers go into a bank, they do not just see the cash sitting on the floor; rather, it is secured inside a vault, which creates another physical layer of security.

High-risk assets typically occupy their own segment, protected by another set of internal perimeter security devices. The security mechanisms may be firewalls or jump servers. Designers will create red (for low-security) and black (for high-security) zones. To move from a red to a black zone, in which high-priority databases reside, the user must go through a jump server. The latter first requires a Remote Desktop Protocol (RDP) session before accessing the database.[5] This creates yet another layer of security in the network.

> “ONE OF THE MOST EFFECTIVE WAYS OF ACHIEVING THE GOAL OF LAYERED DEFENSE IS THROUGH THE DESIGN OF THE NETWORK.”

Proxy

An additional and valuable layer of protection that should be included in a comprehensive layering approach to security is the use of a network proxy or firewall proxy. A content filter at the network level is critical to the overall strategy.[6] Proxies can filter out .exe or .bat files, which can greatly enhance the overall security package. Advanced filters can also filter based on application type and reputation. These filtering databases are typically cloud-based and can be fast to respond to zero-day outbreaks of malware. They can also be highly effective at dealing with ransomware.

An application proxy acts as a gateway between the end-user system and the Internet, essentially hiding and protecting the end point.[7] The user system makes contact with the application proxy, while the proxy communicates, on behalf of the user, with the external server. The latter never has access to the internal network.[8] Although proxy systems alone are not a solution to security, they add a pleasing complement to virus protection and several other layers of network defenses.

> PHYSICAL SECURITY IS NOT MERELY A LAYER OF NETWORK SECURITY; IT NEEDS TO BE LAYERED IN ITS OWN RIGHT.

Third-Party Networks

With security designers so concerned with preventing breaches and virus outbreaks in their internal networks, the security industry has responded by offering solutions that prevent potential malware from ever entering the end user's environment. To complement the implementation of end-point security software and deep-packet scanning at the firewall level, many designers also use third-party networks to scan for threats before the traffic enters the end user's network.

An excellent example of this is email scanning in the cloud using a vendor network. Several vendors offer this service, including Barracuda and Appriver. The design requires email sent to the end user to be diverted to the third-party network, where it is scanned for viruses, phishing, spam or many other combinations of filters. Any potential threats are removed before the clean email is sent to the end user's internal servers. These security solutions are extremely granular and very quick to respond to outbreaks.

An added benefit of this service is that traffic bound for the internal email server is reduced significantly. According to statistics, more than 69 percent of emails sent in 2013 were either spam or viruses.[9] The number of spear-phishing email campaigns increased by 91 percent in 2013 over the year before, indicating that attackers had become more sophisticated in their assaults. They are learning about the end users and targeting specific individuals deemed to be high-value targets.[10] With that type of statistic, the added layer of passing the Internet traffic through a third-party network where the traffic can be scanned for threats is of high value in a layered-security approach (**figure 3**).

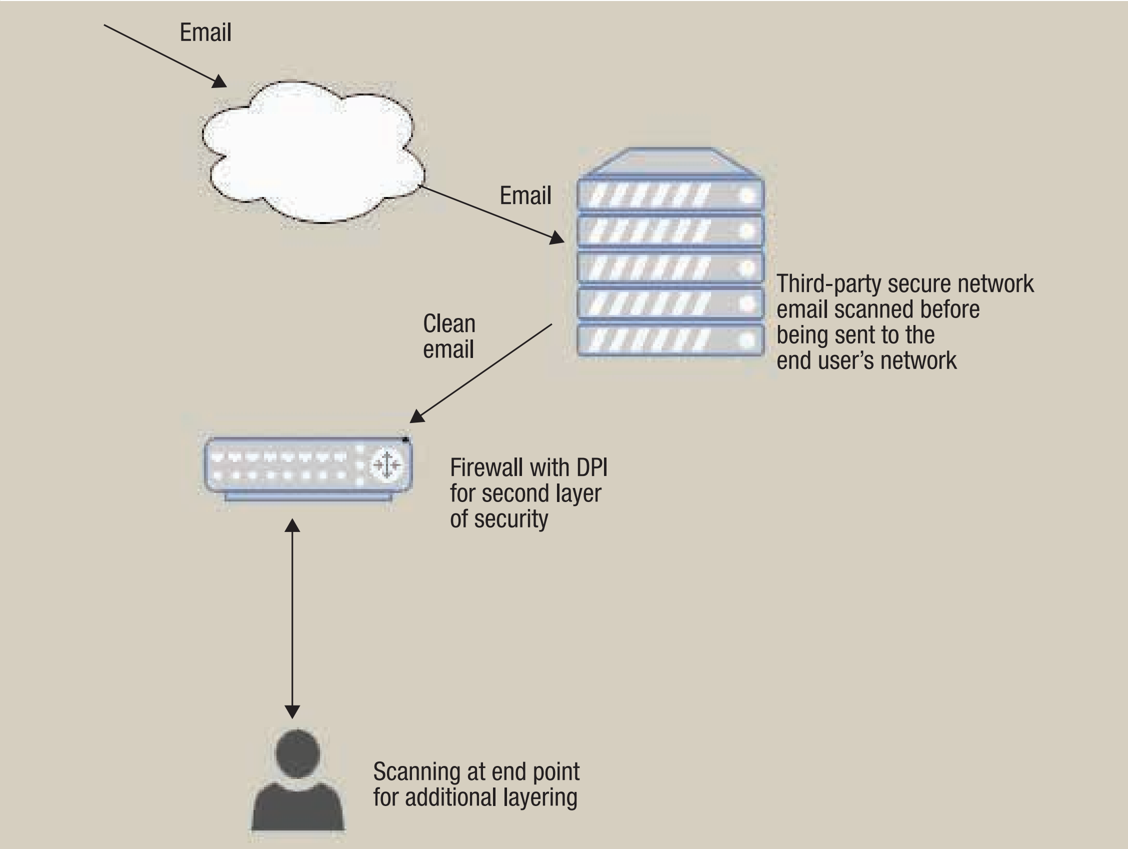
Physical Security

Although the need for physical security may seem obvious, it can all too easily be overlooked. It makes no sense to have a layered approach to network security and neglect the physical aspect.[11] Physical security is not merely a layer of network security; it needs to be layered in its own right. For example, one key that allows access to the server room, or one camera that records entry to the building, is not sufficient. Access to the building should be restricted and monitored, just like the network infrastructure. If someone compromises the network from the outside, the organization's mechanisms should alert employees and allow them to establish what information was compromised and for how long.

Physical security should serve the same purpose: If someone compromises the physical security, resources should be in place to tell who breached the defenses, when and where. This is done by deploying security guards where possible and having keyed and logged access to the building, including separate access to sensitive areas such as the data center. Access to the building should be recorded via a camera system, while a separate system should monitor access to sensitive areas.

These components, just like network logging, should be reviewed on a regular basis. It is not advantageous to have cameras in place if no one is reviewing them, nor to have electronic card access

Figure 3—Third-Party Network Layering


Email
Email
Clean email
Third-party secure network email scanned before being sent to the end user's network
Firewall with DPI for second layer of security
Scanning at end point for additional layering

if the logs are not evaluated. Alerts should also be configured to rouse security personnel regarding any failed attempts to access the building or sensitive areas. In sum, physical security is a key component of a layered security implementation.

Authentication

Authentication is the process of proving that people are who they say they are. This procedure is at the core of every security system in use today. As discussed in this article, these systems have layers of protection to keep people who are not meant to be there, or to have access, out of the network and away from data. These processes cover the back doors and prevent the infiltration of malware. Authentication is the process of allowing permitted access through the front door of a network. This operation must also be layered, just like other sections of the network. How is this accomplished? By using multifactor authentication (MFA). "The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a computer system or network."[12] Every authentication system can be compromised and should not, particularly those with high-value assets (e.g., banks, power plants), rely on a single form of authentication.

> “AUTHENTICATION IS AT THE CORE OF EVERY SECURITY SYSTEM IN USE TODAY.”

Designers can use several options to achieve MFA. These can be broken down into three categories: something one knows (a password), something one has (a token number or code sent via email or text), or something one is (biometric). Security designers combine two or more of the three categories to create MFA. The procedure is effective only when

two or more passwords are required. For example, a person accessing a financial database may be required to enter a password (something he/she knows), then enter the code from a smart card (something he/she has), and may still be required to scan a fingerprint or iris for access. Following this process allows for layered security during authentication.

> “BUILDING DEFENSES, SETTING ALARMS AND MONITORING IS NOT ENOUGH—IT IS NECESSARY TO CONSTANTLY TEST THE DEFENSES.”

User Education

With the increase in social engineering and zero-day attacks, user education plays a huge part in a layered security approach. The end user may be the final or first (depending on where the attack originates) line of defense. To ignore the user would be a massive mistake. With script kiddies becoming more prevalent, these amateurs can easily circumvent firewalls by sending mass emails in an attempt to persuade users to click on loaded links; the user must be aware of the risk. According to one expert:

> *A strong security architecture will be less effective if there is no process in place to make certain that the employees are aware of their rights and responsibilities. All too often, security professionals implement the ‘perfect’ security program and then forget to factor the customer into the formula.*[13]

Testing

The final step in any sound security design is the testing phase. Routine testing should be a matter of written policy and followed to the letter; network security officers should look at themselves as military personnel and be constantly prepared for an attack. Building defenses, setting alarms and monitoring is not enough—it is necessary to constantly test the defenses. Such testing must be performed both internally and externally, by internal staff and outside security experts. “Penetration testing is like having a mock firefight on a military base.”[14] White-hat hacking, penetration testing and vulnerability testing are crucial in a layered security approach to network defense.

Conclusion

With the increase in data breaches and the resultant cost to organizations, the protection of networks and data is paramount. Firms cannot afford to turn a blind eye to network security. Organizations are increasing their security spending, and in many cases these additional resources are going to add layers of defensive mechanisms.[15]

Security designers are using various approaches to layering defenses to thwart hackers and prevent data loss. They are implementing layers to prevent malware infections and head off hackers at the border, and increasing the complexity of network design to add additional passes through checkpoints for data access. Designers are also routing traffic through third-party security networks before entry into the trusted network to weed out threats before they ever enter the network.

Those in charge of physical security, meanwhile, are implementing layered security in their design and complementing network-based layered security. The process of MFA is quickly becoming *de rigueur* in the move to standardize the process of a layered defense. Security officers are educating their user base as well as using mechanisms to test the effectiveness of their programs.

Policy design and implementation are crucial in designing and implanting layered security. The security policy of modern networks is to mandate many layers of data scanning before entry and/or exit from the network. Although these methodologies will not prevent all data loss, with the concept of layered security becoming the norm, they will play a significant role in protecting the networks of today and tomorrow.

Endnotes

[1] Perrin, C.; "Understanding Layered Security and Defense in Depth," *TechRepublic*, 18 December 2008, *https://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/*

[2] Federal Communications Commission, "Cyber Security Planning Guide," USA, p. 3, *https://transition.fcc.gov/cyber/cyberplanner.pdf*

[3] Choi, Y. B.; C. Sershon; J. Briggs; C. Clukey; "Survey of Layered Defense, Defense in Depth and Testing of Network Security," *International Journal of Computer and Information Technology*, vol 3, issue 5, September 2014, *https://www.ijcit.com/archives/volume3/issue5/Paper030518.pdf*

[4] McGuiness, T.; "Defense In Depth," SANS Institute, 2001, *https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525*

[5] Williams, J.; "Practical Threat Management and Incident Response for the Small- to Medium-Sized Enterprises," SANS Institute, June 2014, *https://www.sans.org/reading-room/whitepapers/analyst/practical-threat-management-incident-response-small-medium-sized-enterprises-35257*

[6] Musa, S.; "Five Steps to Take on Ransomware Using a Defense-in-Layers Approach," Government Technology, 14 April 2016, *www.govtech.com/security/5-Steps-Ransomware-Defense-in-Layers-Approach.html*

[7] Roesler, J.; "Defense in Depth Layer Six: Application Security," Topics on Information Security, 6 February 2013, *http://infosectopicsbyjen.blogspot.com/2013/02/defense-in-depth-layer-6-application.html*

[8] Dominguez, J. A.; "An Overview of Defense in Depth at Each Layer of the TCP/IP Model," SANS Institute, 2002, *https://www.giac.org/paper/gsec/2233/overview-defense-in-depth-layer-tcp-ip-model/103817*

[9] Symantec, *Internet Security Threat Report 2014*, *www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf*

[10] *Ibid*.

[11] Banathy, A.; G. Panozzo; A. Gordy; J. Senese; "A Layered Approach to Network Security," Industrial IP Advantage, July 2013, *www.industrial-ip.org/en/knowledge-center/solutions/security-and-compliance/a-layered-approach-to-network-security*

[12] Mohamed, T. S.; "Security of Multifactor Authentication Model to Improve Authentication Systems," *Information and Knowledge Management*, vol 4, issue 6, 2014, *www.iiste.org/Journals/index.php/IKM/article/viewFile/13871/13939*

[13] Peltier, T.; H. F. Tipton; M. Krause; *Information Security Handbook, Fourth Edition*, Auerbach Publications, USA, 2002

[14] *Op cit* Choi *et al*

[15] Filkins, B.; "IT Security Spending Trends," SANS Institute, 2016, *https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697*