Global Information Assurance Certification Paper

Tiered Security in the Enterprise Network

By: Thea Barnes
Version: 1.2F

Introduction

'Enterprise Network' -one of the most popular high-tech buzz terms of the millennium and, conceptually, the deliverance that many institutions have long awaited as the answer to all of their Information Technology (IT) System security fears. And now, still at the infancy of a revolution believed to dwarf that of the Industrial Revolution hundreds fold, the IT industry is best suited to tackle security issues in their primal state as the nature of the field dictates that is the best time to do so anyway. Industry recognition of this fact and ability to employ the assets for accomplishment makes doing so an even more practical reason. But to fully understand the role of the Enterprise Network in the task of securing electronic information use and exchange, means defining the Enterprise Network, what comprises it, who it best suits, its capabilities, its limitations, its upkeep, etc. The variables are unlimited but all can be included into a set number of subcategories. The Enterprise Network, defined in its most primal form, is a multi-layered, cross- platform series of high-tech security features that are seamlessly interconnected across various platforms and infrastructures with the objective of providing the greatest possible protection to the institution, and its users, for which it is designed to. The security aspect of this concept is that of a defense-in-depth approach. Each individual layer, or tier, can itself be thought of as being a network, complete with hardware, software and mediums of connectivity. Hardware components included in each layer may be firewalls, VPN Gateways, routers, load balancers, and intrusion detection modules (IDSs). All of these have operational software associated with them. In addition, some software residing at the network boundary may actually be a specific application that is a designated component of protection. So to fully understand the Enterprise Network and avail oneself to the strongest level of protection it affords would require the analysis and understanding of the different tiers, or boundaries, with respect to the objective of the institution employing its service and the reasons for connecting the different layers. As the popularity of Enterprise Networks has grown, not only do they include the interconnected sub-areas within the organization and long haul connectivity, but many companies permit access to their networks by business partners of the organization and by customers. This carries transacting far beyond traditional network boundaries and along with that it introduces additional security risks. Allowing network users access to critical data while maintaining the integrity of the system is one of the major obstacles facing successful implementation of the Enterprise environment. IT professionals often have to employ network segmentation and access controls methods to accomplish this, thus creating boundaries.

Background and History

In the early 1990s when the PC started becoming a common fixture in any office or household, it was commonly a 'standalone' and for the public, the internet was still a basic unknown. The internet was used mostly by the government, education institutions, and by 'geeks' employing bulletin boards for exchanging ideas with other 'geeks' on topics of interest. By the mid to late 1990s many businesses, large and small, began to see that maybe there was commercial advantage to electronic information exchange. The growth from innovation from businesses has spread to usage of information exchange in the common household. But like anything else this growth has been accompanied by problems involving exploitation, intrusion and abuse. Although threats against legitimate causes are age old, the rapid and far-reaching emergence of the

information age has brought about issues on threat management the likes which had never before been imagined, let alone researched. The past six to eight years have brought the need for IT, and thus security, to the forefront of any venture that expects to be successful. Many people do not even have to leave their homes because of the conveniences brought about by modern electronic information exchange. Among other things, people are able to work, shop, bank, and educate themselves all from their homes, via internet connectivity. In the early commercialization of this evolution, many resourceful individuals and businesses imagined being able to conduct those activities from home and knew the profit potential that each could offer, provided those who demand it feel secure engaging in this activity. Communications oriented businesses have studied the needs of those using electronic exchange and have collaborated on this issue to determine how to best serve the user needs. The early implementation of the electronic exchange of information was rather crude by comparison with today's secure and heavy-duty capabilities. Many of the amenities of today were not available then, but they evolved from that early technology to what they are able to do today and to what can only be imagined in the future. The specifics involved in reliable, effective and seamless IT implementation, and the associated security, have given way to the birth of the popularity of the Enterprise Network. The concept of the Enterprise Network is the provision of layered architecture and security that many institutions have decided best fit their operation and security needs.

Enterprise Security, an Overview

Enterprise Security is a term that generalizes the collection of technologies that are incorporated to perform a specific task in a secure manner. Usually the implementation and maintenance of such an endeavor requires the employment of a group of qualified IT professionals to assure success. IT professionals begin the task with assessing the objectives of the institution wishing to employ the network. This includes interfacing with the organization's senior management or anybody in a position to allocate the money for the project. Other issues the IT professionals would have to assess would be the geographical size which the network will cover- a room, a floor, a building, a campus, a local area network (LAN), a metropolitan area network (MAN), a wide area network (WAN), across country, or globally. And how can something ranging from such possible extremes be secured consistently? What will the Enterprise Network cover logically? Will the Enterprise Network have to be expanded? Will it have to include the integration of existing IT appliances? How will compatibility issues then affect the security of the information electronically exchanged? How will all of this be susceptible to threats and unauthorized access? How will continued assessment of threats be approached?

The mere implementation of an Enterprise Network is an inference in itself that the network will cover a large area geographically and will employ the use of communications lines provided by a commercial carrier to complete their long range connectivity needs over the internet in a secure manner. This usage of commercial, publicly available lines poses security risks. It manages have to carefully examine the potential threats in usage of these facilities. Additionally, vulnerabilities inherent to the system itself have to be studied The Enterprise Network often finds solutions to these issues through two primary means, the use of a Security Plan and through the understanding Risk Management needs.

Threat and Vulnerability Assessment

Threat & vulnerability assessment is conducted in an effort to investigate existing threats to the system and to assess vulnerabilities, both intentional and unintentional events, caused by a variety of inherent factors. Common inherent factors include human error, component failure, system design flaws, patches and updates, environmental threats (physical and logical), and generic threat information. Threat and vulnerability assessment is a crucial part of the successful implementation of an Enterprise Network. Threat assessment mainly involves awareness of current industry trends and the patterns that lend themselves to intrusion. It may require the IT security professional staying abreast of the commercial IT products in an effort to determine the best way to integrate such products with the companies existing infrastructure. IT Security professionals are able to assess the vulnerabilities of a system through different means. State-of-the-art analysis software, sophisticated techniques, industry knowledge and a proven methodology are some of the best methods available to assist system administrators to develop ways to ensure that system operation is not interrupted. Protecting a company's network through the use of systems that alert an administrator to vulnerabilities in the system they are monitoring, in real-time, permits administrators to take immediate action. Additionally, if an organization is able to employ security specialists, greater vulnerability assessments can be made that may include susceptibility to a variety of attacks that are commonly used to deface, destroy or compromise critical data and files. Some common forms of attack that may be assessed include hidden field manipulation, cross-site scripting, and forceful browsing. Prevention steps that IT administrators may use include: implementation of strategic security controls, disabling vulnerable features and repairing weaknesses to effectively combat the risks that exist in your network.

Security Policy and Risk Management

Almost as soon as the initial proposal of the Enterprise Network comes, so does the Security Policy. This means that at one of the earliest stages of assessment a Security Policy will have to be established through the collaborative work or the management team and the IT professionals implementing it. A Security Policy is a document that outlines the general expectations of the network as well as promulgates requirements that the network has to meet. Security policies are set for all stages of the network, involving both logical and physical descriptions of connectivity. Security Policies are often peculiar to certain domains or components of the network, allowing them to be implemented in the most effective manner. Since the Enterprise Network is inclusive of both internal and external functions, security domains provide an added layer of defense.

Another inherent issue characteristic of the Enterprise Network is that of Risk Management. Risk Management entails the study of the 'potential' threat that the network may be susceptible to. Since the complete elimination of threat is an unreasonable expectation, if not actually impossible, it only makes good practical business sense to fully analyze the threats. Through an effective risk management program, the management can assess their resources and allocate those they feel are best suited in roles covering the analysis of such threats. Some of the issues requiring the attention of Risk Management include the analysis of past system attacks and how

they occurred, an industry study of the different vendor products and how they handle threat, and the size of the Enterprise Network that will be implemented.

Architecture of Tiered Networks

From a functionality standpoint, the success of the enterprise network is entirely dependent upon design, or the architecture of it. Once the IT professionals have ascertained the managements realistic objective for the network and understand budget limitations, they are in a position to determine the best way to go about implementing it. This process requires a reasonable assessment of the available security and technology to meet that objective. With the defense in depth principle in mind, the focus turns to layering and to the positioning of boundaries.

Defining Boundaries

Loosely defined, a boundary is a delimitation of a designated area. In the case of the Enterprise Network and defense in–depth security, the term boundary is somewhat relative since the network is simply a series of boundaries, where the inner or outer-most can be dependent upon the frame of reference in which the observer stands. So when referring to a boundary, it is important that all parties involved define what part of the network is in consideration.

Criteria of a Boundary

In the Enterprise environment, a network boundary is a standard set of protections that define the interface between two network sections. Network boundaries enforce policies that are required to interconnect those networks. They also provide secure mechanisms by which remote access can be successfully made and to which legacy networks may be interfaced. Boundaries also provide an additional layer of protection to communities residing within them. Although network boundaries may be generically defined, doing so is not inclusive of the range of boundary functionality as these examples have illustrated. There are many different functions of network boundaries.

Components at the Boundary

As can be imagined, the network boundaries of the enterprise network as they are defined and centrally located plays a very crucial role in the performance, and ultimately, the success of at least two parts of the broad network. Consequently, the components making up the boundaries are very important. Among common boundary components, you'll often find router and/or switches (depending on data layer desired) dedicated, high-end workstations hosting firewall and web scanner applications, load balancers, intrusion detection modules, and single/ dual sided VPN gateways. Of course, there are cables, either cable or fiber and punch panels or some other form of junction point.

A Look at Boundary Security Components

Although all of the components of the network boundary have an essential function, there are some components of the network boundary of the enterprise network whose sole purpose is to provide a greater amount of security to the network which resides behind it. These components can even be doubled up, at times, depending on their position in the network and the maximum amount of traffic that is expected to pass through the boundary. An example of this could be dual firewalls, set up in parallel, at the boundary. The following is a list of some of the most critical components likely found at a boundary of an Enterprise Network.

Routers, a necessary component of any network boundary, provide a relatively strong layer of protection. As the name implies, their primary duty is to route traffic; however, since they do this based on the IP and packet information of traffic attempting to enter or exit the network, their internal tables can be configured to deny passage to some traffic whose IP or packet characteristics match what the router is configured to do. The router filters network traffic in this manner and in the process provides a layer of protection, albeit a weak one. Although there are ways in which this system can be fooled, the initial protection it offers is better than nothing.

The firewall, another essential network boundary security component in the enterprise network, is commonly nothing more than a high –performance PC that runs an application that performs packet filtering in a manner similar to the way a router does, only more intricately. Most modern, popular firewalls provide the user with a Windows style interface, thus providing the administrator a familiar setting. Through the configuration of settings called rules, firewalls can be configured in ways that can create filtering of both inbound and outbound data packets. Firewalls implemented into enterprise networks analyze the requests and responses of protocols and determine if their behavior is in accordance with RFC standard or if the traffic is rogue.

An Intrusion Detection System (IDS) is a security mechanism residing at a network boundary whose function is to monitor and analyze network traffic and events for the purpose of detecting unauthorized attempts to access a network. In the enterprise environment, the IDS analyzes the packet data streams within the network and searches for suspicious activity. This vigilance often allows system administrators to respond to security breaches before a system is compromised. Most enterprise IDS systems have alarms that sound if suspicious activity is detected. A management console, part of the IDS, receives the alarm as well as any details of the event that triggered.

A VPN Gateway is a device used in a Virtual Private Network (VPN) that performs encryption and decryption of data. Through this device, IP traffic is able to travel securely over a public TCP/IP network because the data is encrypted from one end to another. A VPN uses a method "tunneling" to encrypt all IP data. In the Enterprise Network, VPNs use advanced encryption and tunneling to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets and the gateway devices reside at the network boundary.

Different Boundary Functions

One of the most common network boundary types is the one where a local area network interfaces with long-haul transport, or a commercial carrier line, like AT&T or Sprint. Security mechanisms are placed at this interface as a way to secure data, either into or out of, a section of the network. These mechanisms include software application and configurations and hardware. The Enterprise Network benefits from this by using the mechanisms that will preserve operational integrity without hindering performance or end user operation. Since most enterprise networks will be required to perform at 100% of their ability around the clock, mechanisms must be employed that will be able to analyze, and cross analyze what happens at the boundary. This is done with simplicity kept in mind.

The boundary at which one may find a separate community, residing within the outermost network boundary of a LAN, will often find that the interface delimiting the two is rather seamless. Although security is a factor here, it may be less so than at other boundaries that interface with a completely external network. The hardware components found here will most likely be routers, switches, and possibly an encryption device. This inner community may even be considered a sub-net of the LAN and be so defined logically only.

Because most existing computer infrastructures within large organizations contain significant corporate assets, including the business rules, processes, and information required to run a business, enterprise networking has to be integrated with this infrastructure in a cost effective manner to prove its worth. Companies with significant legacy infrastructures have to leverage these assets when pursuing e-business initiatives, such as the integration with an enterprise network, into the corporation. The type of boundary interfacing a legacy network and an enterprise network should contain security features appropriate for today's electronic environment. Traditional integration methods have often required code modification, or interfacing, at the system's programming or application interface level. Security components integrated at this level would include the protocol gateway. Additionally a transcoder can is integrated to provide broadcasting, synchronization, caching, and encryption features between the legacy system and the enterprise. This kind of integration is often a complex and tedious task for developers and administrators and its size can increase substantially if the number of legacy applications and sites is high. The ability of a company to utilize its legacy applications while still moving forward with new enterprise technology can be difficult in the implementation stage. But with the rapid advancement in communication, they really have no choice but to make the integration, and bear its potentially high cost, if they want to compete in the global marketplace.

Bandwidth capacities at the boundary interface can be an issue and is dependent upon the size and expectancy of the throughput capabilities on each side of the boundary. Connections from commercial carrier lines may be in the range of T1 to 0C-3. Core infrastructure of the network delimited by the boundary normally does not affect the bandwidth where the boundaries interface. However, if the bandwidth capabilities vary, especially by a large amount, the side

with the lesser capability most likely will be incapable of keeping up with the data transfer of the network on the other side of the boundary, or at best have its performance significantly slowed. Many popular commercial products especially designed for the integration of legacy components with those of the Enterprise contain settings to allowing seamless interfacing of the two, however, an experienced professional would be best suited to perform the installation of products of this type.

Conclusion

The Enterprise Network is a modern networking concept utilizing a series of security mechanisms for advanced protection in the exchange of electronic information. What also makes the enterprise network attractive is its ability to integrate, often seamlessly, with legacy infrastructures so that usage of them is not obsolete. Additionally, the enterprise concept employs commercial communications lines in the transference of data in long haul executions. In the security layers comprising the Enterprise Network, interconnecting boundaries often contain the most advanced security mechanisms of the network. Common security components contained therein often include routers, VPN gateways, intrusion detection system modules, and firewalls. Although each component has a unique security oriented role in the architecture, implementing all of them in an efficient manner will afford the greatest protection. To accomplish the integration of all these components, a team of experienced IT professionals must be employed. Success of the implementation also includes cognizance of industry trends in security and security breaches. Knowledge of this activity allows the network administrators to know how maintenance, upgrades, and modifications to the network can be most effective. This is another area in which the experience of IT professionals is needed.

As internet use and demand continue to grow, corporations, governments, universities, etc will continue the expansion of their networks with new technologies and employ new e-commerce applications. Along with this, network security will continue its vital role in preventing the intrusion, exploitation and attack of systems. Additionally, the management of network security vulnerabilities to help ensure that use of these networks is worry free and reliable. In many cases, the best of these networks will be Enterprise Networks comprised of tiered security mechanisms.

References

Cisco, "Overview of Routing between Virtual LANS" copyright 1989-1997, http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/switch_c/xcvlan.htm (2 Jan. 2002).

Carnegie Mellon University, Software Engineering Institute, "The Survivable Network Analysis Method: Assessing Survivability of Critical Systems", http://www.cert.org/archive/pdf/sna-short.pdf (2 Jan. 2002).

Brooke, Paul, "Deploy and In- Depth Defense for Deeper Protection", October 2001, http://content.techweb.com/custom/security/1006.html (2 January 2002)

Timestep, Technical Paper, "Understanding the IPSec Protocol Suite" (March, 2000) http://www.timestep.com/doctypes/technewbridgenote/pdf/ipsec_nn.pdf (2 Jan. 2002)

http://csrc.nist.gov/isptg/word97/01Introduction.doc (2 Jan. 2002)

Cooper, Mark. "An Overview of Intrusion Detection Systems" URL:http://www.xinetica.com/tech_explained/general/ids/wp_ids.html (2 Jan. 2002).

http://www.niuf.nist.gov/docs/436-95.html (2 Jan. 2002)

Joint Information Systems Committee, "Purpose of a JANET Security Policy", September 1995.http://www.ja.net/documents/JANET_security_policy.html (2 Jan. 2002)

Federal Information Processing Standards Publication 191, November 1994, http://www.itl.nist.gov/fipspubs/fip191.htm (2 Jan. 2002)