Network Security – A Layered Approach

Kanchan Bala¹, Barjeena Lucky², Surinder Pal Garg³
¹H. I. M. T. Greater Noida, ²D. N. College, Hisar, ³G. P. Hisar.

Abstract

Security issues are critical for the success of pervasive computing. Because pervasive computing and e-business may provide millions of people with the power to move trillions of dollars in goods or money by a few mouse clicks, the security of e-business transaction is a top priority. With the number of security threats on the rise, network security has become an essential part of maintaining the privacy and integrity of an enterprise. Network security provider has the technology to help you define your network against attacks by implementing preventative security solutions. Cryptography is a minor tool to obtain Network Security. Our layered approach to network security was designed with the knowledge that no single tool can protect every segment of network from harming. In reality, the surge of blended threats has resulted in the need for integration between individual security products in order to reduce possible gaps in protection.

1. Introduction

Network layer security is a key aspect of the internet based security mechanism. Originally; people were concentrating only on application level security. However, new security requirements demand that even the lower level data units should be protected. With the view in mind, network security mechanism has emerged and is being used extensively in real life.

Figure 1. Network security – A Layered Approach

Network security is a mission-critical concern for enterprises, government agencies, and organizations of all sizes. Today’s advanced threats demand a methodical approach to network security. In many industries enhanced security is not an option—it’s mandatory federal regulation such as sarbness-oxelyGLBA and other require organizations such as financial institutions, health care providers and federal agencies to implement stringent security programs to protect digital assets.

Now we are introducing you to a layered approach for securing your network. This layered approach is both a technical strategy, espousing adequate measures be put in place at different levels within your network infrastructures. The layered approach centers on maintaining appropriate security measures and procedures at five different levels within IT department.

1. Perimeter
2. Network
3. Host
4. Application
5. Data

Figure 2. The security level in the layered approach and the technologies that function on each.
2. Perimeter Security (Level 1)

The perimeter is the first line of defense from outside, un-trusted networks. The perimeter acts as the first and last point of contact for security defenses protecting the network. It is the area where your network ends and the Internet begins. The perimeter consists of one or more firewalls and a set of strictly controlled servers located in a portion of the perimeter referred to as the DMZ (demilitarized zone). A DMZ typically contains the Web Servers, email gateway, network antivirus and DNS servers that must be exposed to the internet. A compromised network perimeter can cripple your ability to conduct business. For example, if your organization relies on your Web servers for revenue generation, and those servers have been hacked and are off-line, you lose money for every minute they are down. The following technologies provide security at the network perimeter.

2.1 Firewall

A firewall is typically installed on a server connected to the inside and the outside of the network perimeter. A firewall performs three general functions:
1. Traffic Control
2. Address Translations
3. VPN terminations

A firewall acts like a sentry. If implemented, it guards a corporate network by standing between the network and the outside world. All the traffic between the network and the internet in either direction must pass through the firewall. The firewall decides if the traffic can be allowed to flow or whether it must be stopped from proceeding further. It ensures that only permissible requests are allowed through. Additionally, firewalls help secure the network by translating internal IP addresses to IP addresses that are visible to the internet. This prevents the disclosure of critical information about the structure of the network inside the firewall. A firewall can also terminate VPN tunnels.

2.2 Network Based Anti-Virus

Installed in the DMZ, network based anti-virus software compares incoming and outgoing email message content to a database known virus profiles. Network based anti-virus products block infected email traffic by quarantining suspicious and infected e-mail messages and then notifying recipients and administrators. This prevents email infected with a virus from entering and spreading across your network, and it prevents your network from spreading virus infected email. To work effectively, the database of known viruses must be kept up to date.

2.3 VPN

A VPN is a mechanism of employing encryption, authentication and integrity protection so that we can use a public network (Such as the Internet) as if it is a private network. A VPN is a mechanism to simulate a private network over a public network. It essentially creates an encrypted ‘tunnel’ across the Internet, approximating the security and confidentiality of a private network. A VPN tunnel can terminate on a VPN-enabled router, firewall or server within the DMZ. Enforcing VPN connections for all remote and wireless network segments is an important best-practice that is relatively easy and inexpensive to implement.

3. Network Security (Level 2)

The network level of the layered security model refers to your internal LAN and WAN. The following technologies provide security at network level:

3.1 Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

IDS and IPS technologies analyze traffic moving across your network in much greater detail than your firewall. Similar to antivirus systems, IPS and IDS devices analyze traffic and compare each packet to a database of known attack profiles. The difference is that anti-virus inspects files on the system, whereas IDS and IPS inspects packets within network traffic. When attacks are detected, IDS/IPS technologies take action. IDS alert and IPS block the harmful traffic. In fact, most IPSs have an IDS at their core. The key difference between the technologies is implied by their names. IDS products only detect malicious traffic, while IPS products prevent such traffic from entering your network.
3.2 Vulnerability Management

Vulnerability management system performs two related function. They scan the network for source addresses, TCP state verification, and rouge services running on the network. They manage the process of repairing the vulnerabilities found. Vulnerability managers scan devices on a network for flaws and vulnerabilities that could be exploited by hackers or harmful traffic. They typically maintain a database of rules that identify known vulnerabilities for a range of network devices and applications.

3.3 Network access control

Network access control solutions protect the network by ensuring that endpoints meet defined security standard before they are allowed to access the network. Endpoints security solutions allow or deny access based on tests run against a device when it attempts to connect. They typically test for (1) required software, such as service packs, up to date antivirus definitions, etc. and (2) prohibited applications, such as file sharing and spyware.

3.4 Access Control and User Authentication

Access control entails authenticating users who access your network. Authentication is typically performed against the user information in a RADIUS, LDAP or Window ACTIVE directory.

4. Host Security (Level 3)

In the layered security model, the host level pertains to the individual devices, such as servers, switches, routers etc on the network. Each device has a number of configurable parameters that, when set inappropriately, can create exploitable security holes. These parameters include registry settings, services operating on the device, or patches to the operating system or important applications. The following technologies provide security at host level.

4.1 Host based Intrusion Detection System

Host based IDs perform similarly to network IDs-the key difference being that they monitor traffic on a single network device. Host based IDs are fine tuned to the specific operational characteristics of the host device and therefore provide a high degree of protection when properly administered.

4.2 Host Based Vulnerability Assessment

Host base VA tool scan a single network device for security vulnerabilities. Host based VA tools are fine tuned to the device they are monitor. They are extremely accurate and make minimal demands on the host's resources. Because they are configured specifically for the host device, they provide an excellent level of coverage when properly administered.
4.3 Network Access Control

Network access control solutions do double duty, protecting both the network and individual hosts. These solutions continually check the host for harmful applications and infection and also verify that required security measures, such as anti-virus and personal firewalls are installed and up to date.

4.4 Anti – Virus

Device-specific anti-virus applications provide an additional layer of protection when used in conjunction with network based anti-virus tools.

5. Application Security (Level 4)

Application level security is currently receiving a great deal of attention. Poorly protected applications can provide easy access to confidential data and records. The hard truth is that most programmers don’t code with security in mind. Applications are being placed on the web for access by customers, partners or even remote employees with increasing frequency. The following technologies provide security at the application level:

5.1 Application Shield

An application shield is frequently referred to as an application-level firewall. In ensures that incoming and outgoing requests are permissible for the given application. Commonly installed on web servers, email servers, database servers and similar machines, an application shield is transparent to the user but highly integrated with the device on the backend.

6. Data Security (Level 5)

Data level security entails a blend of policy and encryption. Encryption data where it resides and as it travels across your network is a recommended best practice because, if all other security measures fail, a strong encryption scheme protects your proprietary data. Data security is highly dependent on organization wide policies that govern who have access to data, what authorized users can do with it, and who has ultimately responsibility for its integrity and safe keeping. The following technologies provide security at data level:

6.1 Encryption

Data encryption schemes are commonly implemented at the data, the application, and the operating systems levels. Common encryption strategies include PKI, PGP and RSA.

6.2 Access Control / User Authentication

Like network, and host and application level authentication, only authorized users are given to access data.

7. Conclusion

Hackers and cybergang terrorist are launching network attack combines with increasing frequency and sophistication. The traditional approach to security—namely a firewall combined with an anti-virus in incapable of protecting. However, erect a formidable defense by implementing network security using a layered approach.

8. References