Internet Firewalls Essay, Research Paper

Internet Firewalls:

Introduction

The Internet is a complex web of interconnected servers and workstations that span the globe, linking millions of people and companies. But there is a dark side: The convenient availability of valuable and sensitive electronic information invites severe misuse in the form of stolen, corrupted, or destroyed data found therein. Compounding this problem is the unfortunate fact that there are ample opportunities to intercept and misuse information transmitted on the Internet. For example, information sent across telephone lines can not only be seen, but also can be easily manipulated and retransmitted, or software can be developed to do something as fundamental as deny Internet service. Preventing unauthorized access is a cost that should be factored into every Internet equation. What follows is an explanation of Internet security and the concept of Firewalls.

What Makes the Internet Vulnerable?

Let’s look at some of the most common security threats:

Impersonating a User or System – To authenticate Internet users, a system of user-Ids and passwords is used. Anyone intent on gaining access to the Internet can repeatedly make guesses until the right combination is found, a simple but time consuming process made all the easier by programs which systematically try all character combinations until the correct one is eventually generated. User-IDs and passwords can also be trapped by finding security holes in programs; a person looking to abuse the Internet finds these holes and uses the information leaked through them for his or her own personal agenda. Even someone who has been entrusted with high-level network access, such as a system administrator, can misuse his or her authorization to gain access to sensitive areas by impersonating other users.

Eavesdropping – By making a complete transcript of network activity, sensitive data such as passwords, data, and procedures for performing certain functions can be obtained. Eavesdropping is can be accomplished through the use of programs that monitor the packets of information transmitted across the network; or, less often, by tapping network circuits in a manner similar to telephone wiretapping. Regardless of technique, it is very difficult to detect the presence of an intruder.

Packet Replay – The recording of transmitted message packets over the network is a significant threat for programs requiring authentication sequences because an intruder saves and later replays (retransmits) legitimate authentication sequences to gain access to a system.

Packet Modification – This significant integrity threat involves one system intercepting and modifying a packet destined for another system; more significantly, in many cases, packet information can be just as easily destroyed as it can be modified.

Denial of Service – Multi-user, multi-tasking operating systems are subject to denial of service attacks where one user can render the system unusable by hogging a resource or by damaging or destroying resources so that they cannot be used. Service overloading, message flooding, and signal grounding are three common forms of denial-of-service attacks. While system administrators must protect against these types of threats without denying access to legitimate users, they are very hard to prevent. Many denial-of-service attacks can be hindered by restricting access to critical accounts, resources, and files, and by protecting them from unauthorized users. Many invasive Internet opportunities exist for access to corporate and personal information. These instances do occur and care should be taken to guard against them. This is the function of a firewall: To provide a barrier between an Internet server and anyone intent on invading its sensitive data.

Countering the Threat with a Firewall

As the name implies, an Internet Firewall is a system set up specifically to shield a Web site from abuse and to provide protection from exposure to inherently insecure services, probes, and attacks from other computers on the network. A Firewall can be thought of as a pair of mechanisms: one, which exists to block traffic, and the other that exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. A major Firewall benefit is centralized security through which all Internet access must pass, which is far easier to maintain since there are fewer servers to update and fewer places in which to find suspected security breaches. The most important thing to remember is that a Firewall should be designed to implement an access control policy that best fits your specific needs to protect your unique data and resources.

Components of a Firewall

Now, let’s looks at the individual components of a Firewall and how they operate: First, it is important to realize that the term Firewall defines a security concept rather than a specific device or program. A Firewall takes many forms, from a router that filters TCP/IP packets based on information in the packet to sophisticated packet filtering, logging, and application gateway servers which closely scrutinize requested functions. Often firewalls are a collection of systems, each providing a piece of the overall security scheme. Acer has stepped up to the challenge by manufacturing gateway servers for a broad range of Firewall applications. The AcerAltos product family, from the entry-level applications AA900 Single Pentium and AA900Pro Single Pentium Pro servers to the mid-range AA9000 Dual Pentium and AA9000Pro Dual Pentium Pro servers, to the AA19000 Dual Pentium Pro server, fit any size Firewall application. AcerAltos servers can provide the reliability and fault tolerance required by demanding Firewall applications.

Packet Filtering – Accomplished by using a packet filtering router designed to examine each packet as it passes between the router’s input/output interfaces, services can be limited or even disabled, access can be restricted to and from specific systems or domains, and information about subnets can be hidden. The following packet fields are available for examination:

+ Packet type – such as IP, UDP, ICMP, or TCP

+ Source IP address – the system from which the packet was sent

+ Destination IP address – the system to which the packet is being sent

+ Destination TCP/UDP port – a number designating a service such as telnet, ftp, smtp, nfs, etc.

+ Source TCP/UDP port – the port number of the service on the host originating the connection

The decision to filter certain protocols and fields depends on the site security policy; i.e., which systems should have Internet access and the type of access permitted. The Firewall’s location will influence this policy; for example, if a Firewall is located on a site’s Internet gateway, the decision to block inbound telnet access still permits access to other site systems, or, if it is located on a subnet, the decision to block inbound telnet to the subnet will prevent access from other site subnets.

While some services such as FTP or telnet are inherently risky, blocking these services completely may be too harsh a policy; however, not all systems, though, require access to all services. For example, restricting telnet or FTP access from the Internet to only those systems requiring such access can improve security without affecting user convenience. On the other hand, while services such as Network News Transfer Protocol (NNTP) or Network Time Protocol (NTP) may seem to pose no threat, restricting these protocols helps create a cleaner network environment, thereby reducing the likelihood of exploitation from yet-to-be-discovered vulnerabilities and threats.

Unfortunately, Packet Filtering routers suffer from a number of weaknesses: The filtering rules can be difficult to specify; testing must be done manually; the filtering rules can be very complex depending on the site’s access requirements; and no logging capability exists, thus if a router’s (lack of) rules were to still let dangerous packets through, they may go undetected until a break-in has occurred. In addition, some routers filter only on the destination address rather than on the source address.

Event Logging-Used to detect suspicious activity that might lead to break-ins, a host system with packet-filtering capability can more readily monitor traffic than a host in combination with a packet-filtering router, unless the router can be configured to send all rejected packets to a specific logging host. In addition to standard logging that would include statistics on packet types, frequency, and source/destination address, the following types of activity should be captured:

+ Connection Information to include the point of origin, destination, username, time of day, and duration.

+ Attempts Use of Any Banned Protocols such as TFTP, domain name service zone transfers, portmapper, and RPC-based services, all of which would be indicative of probing or attempts to break in.

+ Attempts to Spoof Internal Systems to identify traffic from an outside system attempting to masquerade as an internal system.

+ Routing Re-Directions to identify access from unauthorized sources (unknown routers).

A downside to logging is that Logs will have to be read frequently. If suspicious behavior is detected, a call to the site’s administrator can often determine the source of the behavior and put an end to it, however the Firewall administrator also has the option of blocking traffic from the offending site.

Application Gateways-Also referred to as Proxy Servers. A site would use an application gateway server such as an AcerAltos server to provide a guarded gate through which application traffic must first pass before being permitted access to specific (pre-defined) systems. These gateway servers are used in conjunction with packet filtering and event logging to provide a higher level of security for applications that are not blocked at the firewall; examples include telnet, FTP, and SMTP. They are located where all traffic is destined for a host within a subnet; data is first sent to the application gateway, and any traffic not directed at the application gateway will be rejected via packet filtering. The application gateway then passes authorized traffic to the subnet, rejecting all unauthorized traffic. Here are a number of advantages over the default mode of permitting application traffic to pass directly to internal hosts:

+ Information Hiding – The names of internal systems are not made known via DNS to outside systems; only the application gateway host name is made known.

+ Robust Authentication and Logging – Application traffic can be pre-authenticated before it reaches internal hosts and can be logged more effectively than standard host logging.

+ Cost-Effectiveness – Third-party authentication or logging software/hardware need be located only at the application gateway.

+ Less-Complex Filtering Rules – The rules at the packet filtering router are less complex than if the router needed to filter application traffic and direct it to a number of specific systems; the router need only allow application traffic destined for the application gateway and reject the rest.

Note that an application server is application specific; to support a new application protocol, new proxy software must be developed for it. Several proxy application tool kits have been developed and can be used as a starting place to develop your own gateway software. Alternatively, packages have appeared on the market that offers a complete solution in lieu of costly development time.

An application gateway is the focal point of all traffic to and from the Internet. Selecting the proper server hardware is critical to efficient, reliable Internet access.

Underestimating the load with a server too small produces bottlenecks that affects every Internet user, while overestimating the load with a server too large wastes money, which affects the corporation. Acer has effectively addressed this problem with a broad range of servers and upgrade options. Selecting the proper server is made easier because of the inherent flexibility of the AcerAltos product line — from the uni-processor 133MHz Pentium AA900 and the 180MHz/256KB / 200MHz/256KB Pentium Pro AA900Pro to the dual-processor 166MHz Pentium AA9000 and the 200MHz/256KB Pentium Pro AA9000Pro and AA19000 models — offers the appropriate level of power that best fits the application. The expandability and scalability of the AcerAltos product line ensure incremental growth and performance improvement with minimal cost.

Other Technologies-There are other emerging technologies that, while not new, are just now gaining recognition and standardization. Certain industry niches such as financial services require a higher degree of security. It is imperative for these companies to maintain the safety of financial data and build customer trust; Internet transactions must be made as safe, if not more, as traditional transactions. To do this, these and other organizations have begun relying on two closely linked technologies: Authentication and Encryption. An application of encryption, which further enhances privacy, is the Virtual Private Network (VPN).

Authentication is the process in which the receiver of a digital message can be confident of the identity of the sender and integrity of the message. Authentication protocols can be based on secret key cryptosystems or public key signature systems. Secret key cryptosystems use a key or seed to encode data transmitted over the Internet. Once encoded by the sender, it takes the same or different key to decode it on the receiving end. Only the sender and the receiver know the keys. Should an unauthorized person intercept the message, it is unreadable and nearly impossible to decode without a great deal of time and a powerful computer.

Public key technology uses the concept of digital signatures to assert that a named person wrote or otherwise agreed to the document on which the signatures appear. The signature is an unforgettable piece of data allowing the recipient, as well as a third party, to verify both that the document did originate from the person who signed it and that the document has not been altered since it was signed. A secure digital signature system thus consists of two parts: a method of signing a document so that forgery is unfeasible and a method of signature verification. Moreover, secure digital signatures cannot be repudiated; that is, the signer of a document cannot later disown it by claiming it was forged, since each digital signature is registered with a Certificate Authority.

Encryption has been used by governments and individuals to develop systems for coding, or encrypting, sensitive secrets with the intent to keep them from prying eyes. The science of cryptography involves establishing an encoding key (used for Authentication; see above) consisting of random letters and numbers. Prior to transmission, this key is used in a mathematical formula to change every letter and number in the message. On the other end the receiver then reverses the mathematical process by applying the key to the encrypted message to restore it to the original version. Should someone intercept the message, it would appear as a meaningless series of characters. The length of the key affects how secure the message is; the longer the key, the harder it is to decipher the message. Encryption keys used in today’s commercial systems are between 40 and 128 bits long.

Today’s cryptography techniques and computers, which perform millions of calculations per second, have brought encryption to the point at which the US government cannot break many computer-encrypted documents. Any software using 40-bit or less keys can be exported; software using larger keys is not exportable and must remain in the US.

The combination of sender authentication and data encryption virtually insures the security of sensitive data transmitted over the Internet. Standards for applying these technologies to the Internet are just emerging and have yet to gain wide acceptance. Once they do, however, conducting business on the Internet will be even more secure than in-person transactions.

Virtual Private Network (VPN) technology is being included in some of the more advanced software systems today and provides an added measure of security. Using encryption techniques, VPN hides the content and true source and destination of sensitive data, making it invisible as it moves across the Internet. This technology is also called tunneling because it effectively creates a tunnel through the Internet preventing outsiders from seeing the data.

Conclusion: Plan for Abuse

Planning for abuse before it can happen is the key to building a secure and successful Internet environment. Filtering and connectivity policies must be defined and must incorporate not only security needs, but also the computing needs of the organization. If the computing needs are ignored or short-changed, the Firewall may become too complex to administer or may become essentially useless. Security requirements need to be weighed carefully and accommodations may be necessary if productivity will be hampered by the security policy.

An important concept to remember is that a Firewall should be viewed as an implementation of a policy and that policy should never be made by the Firewall implementation. In other words, decisions on what protocols to filter, application gateways, and other items regarding the nature of network connectivity need to be agreed upon beforehand. Making ad hoc decisions after the fact will be difficult to defend, even more difficult to implement, and will eventually complicate Firewall administration to such a degree that it may be abandoned altogether.

Do your research, put your plan together, and then implement the Firewall policies that best suit your unique environment.

References:

Anderson, Michael R., “Internet Security – Firewalls & Encryption”, New Technologies, Inc., January 17, 1998, Article 1, www.forensics-intl.com

http://www.thewall.com/wallx/wallxbrief.html

http://www.gelb.com/\_vti\_bin/shtml.exe/search.htm

http://www.isc.tamu.edu/tamu/firewall.html