# Global Information Assurance Certification Paper

# Firewall Security

**By**

**Mauricio Angée**

**May 19, 2004**

**Practical Assignment v2.0 - GSEC**

# Table of Contents

# Section I. Firewalls Security Architecture

## 1. Abstract

As technology evolves day-by-day and it becomes more sophisticated, we are faced with new challenges to keep systems and information's integrity safe. During the past few years Internet security has grown and the need for data protection from deliberate malicious activities is inevitable. Therefore, complex computer security systems, such as firewalls, IDS (intrusion detection systems) and anti-virus applications are some of the security systems that "must" be implemented today.

This paper will focus on issues related to the understanding, and the developing network security through the implementation of Firewalls. It will also provide an overview of the "functionability" of firewalls, describing how they work and how they can be implemented, based on specific needs, such as protecting information systems from malicious attacks. It will discuss the firewall Architecture and other aspects related with network security, as well as the benefits of having scalable connectivity while ensuring safeguards to maintaining the network's integrity and availability. Firewalls are designed to filter traffic between networks, a protected or "private networks" and the less trustworthy or "public network." Usually a firewall runs on a dedicated device inspecting traffic coming in-and-out a network. The purpose of a firewall is to provide network security controls, to keep unwanted "things" to come inside the network, and safeguard sensitive information by implementing security policies to filter and audit traffic.

The object of this paper is to create awareness, as well as laying the foundation and understanding of basic network security systems, and to provide the necessary information to protect them from compromising the integrity of information and/or against possible malicious attacks.

## 2. Network Security

Traditional security consists on the protection of property, such property could be secure either physically, digitally or both. Network security could be defined as the protection of networks and their services from unauthorized use, or malicious attacks resulting in damage, modification, lost, or disclosure of information as well as affecting the integrity of information that may result in interruption service or performance. Network security involves the coordination of many functions on a computer network, as a result, planning and deploying a good plan should be the first step to achieve data integrity, availability and confidentiality. The main concern is the protection and privacy of information transferred both through private lines (internal company wire), over public telephone networks, and the Internet.

Having a strong security protecting private networks, and similar perimeter physical security protecting the IT site, but there are still significant holes waiting to be exploited. The nightmare of every IT specialist is the continuous fear of an attack or even a breach of security, which lay the threat of accidental or deliberate unauthorized data access that can compromise valuable information.

Even though computers and network security are some of the most advanced and sophisticated technologies. Such technologies (i.e. IDS, firewalls, etc) must be hand-to-hand with good business procedures and social practices policies. Keeping in mind that no matter how advanced and well implemented these technologies are, they are only as good as the methods used and how they're managed.

## 3. Introduction to Firewalls

Firewalls were developed in the early 1990's, but the first references to a firewall known were called RAN92 or Trusted Information Systems. When a private network is connected to the Internet, that network is physically connecting to thousands of unknown networks and all of their users, Once the link is made, is like an open door to access information, but this connection also provides big opportunities for data sharing, and most private networks contain some information that should not be shared.

A firewall could be defined as a system or combination of systems that enforces a boundary between two or more networks. More explicit is a gateway that filters and limits information coming or going through the Internet connection into your computer systems or private networks. Firewalls are managed by "local security policies" to watch the traffic and grant or deny access to and from network

resources. Firewalls, today, could be application proxies, packet-filtering or a combination of (Pfleeger, C & Pfleeger, S "Security in computing" Pg. 541).

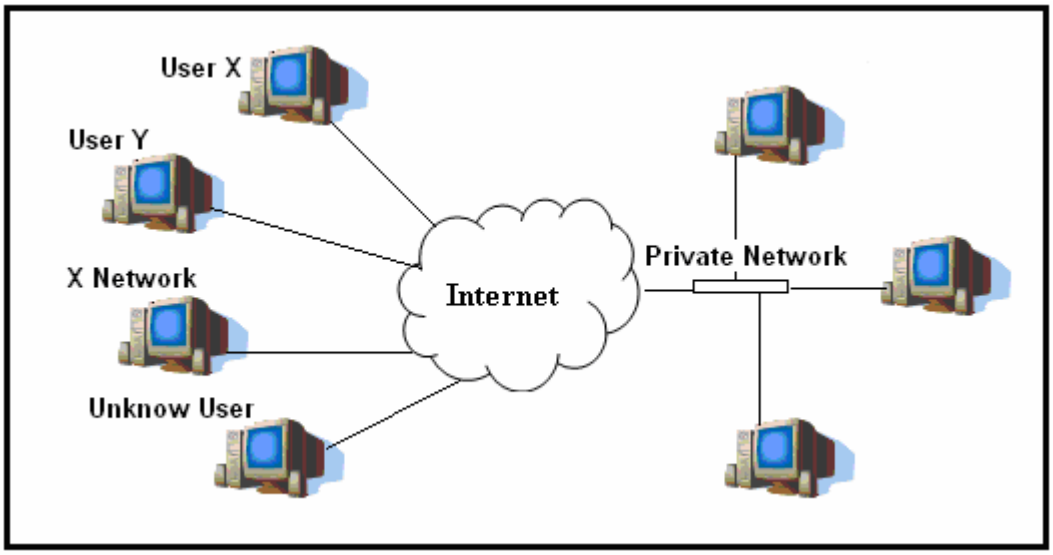


**Figure 3.1 Private Networks – Unprotected Internet connections**

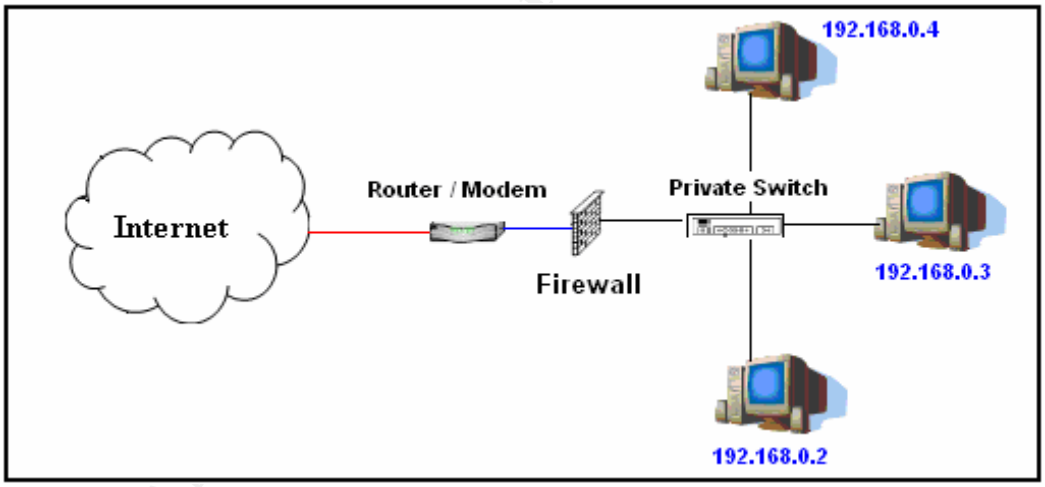


**Figure 3.2 Private Networks behind Firewall**

The most important step in the firewall implementation process is to design and develop a security plan, and always keeping in mind that the strategic planning and the architectural design are often subject to changes or adjustments.

The rapid changes in technology and the many unlawful activities going-on every second, makes networks security a crucial requirement. Today's market offers a wide variety of security solutions, ranging from software based security products (i.e. Norton's Zone Alarm) to complete hardware appliances (i.e. DLink DFL-80).;

Which makes choosing the right solution a lengthy and at times confusing task. With such as wide variety of products in the market, ranging the “right” or the “complete” security solution, finding a solution that is appropriate to cover all the necessary requirements should be the goal. Depending on the application and how it is design, firewalls use one or more of three methods to control traffic flowing in and out of the network.

- **Packet filtering**
  Packets (small pieces of data) are analyzed against a set of predefined filters. After being analyzed, those packets that make it through the filters are checked and sent to the system making the request, and all others packets are discarded (Cisco Systems “Why you need a firewall.” http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch2.htm).

- **Proxy service**
  A request is made to an Internet service from a user (web page). The information is checked by the system, if it passes filtering requirements, the proxy server, returns it to the user without needing to forward the request to the Internet, otherwise the request is terminated.

- **Stateful inspection**
  Stateful inspection trace each connection that passes through all interfaces of the firewall and makes sure they are valid. A stateful inspection firewall monitors the state of the connection and compiles the information in a state table (“state” means that a table remembers the information contained in packets and configuration settings that go from one packet to another.)

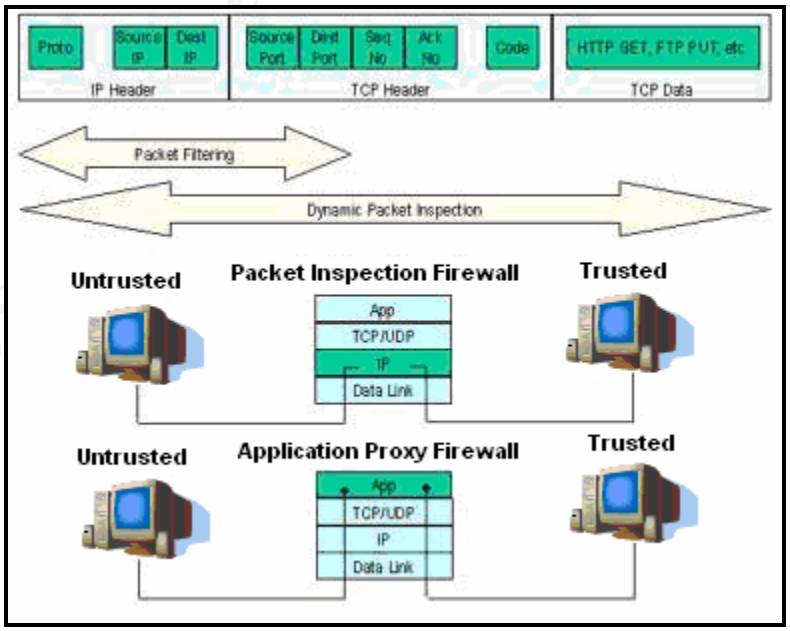


**Figure 3.3 Stateful Inspection Filtering**

Stateful inspection works as follow: a Client computer initiates a request to a Server and sends an IP packet with the source, destination address and ports. The Server receives the request, and then modifies the packet, replacing the source address and port with its own internal address; it also changes the destination IP address to the address of the real server. The Server adds the source, destination ports and addresses into its own ***table*** to keep track of the conversation. The Server sends the modified packet to the internal server. The internal Server responds to the request as the destination address. Server receives the packet from internal server and looks in its table, which maps to the client's. Server then modifies the packet and replaces the server's source IP address and port with its own source IP address and port. Server then changes the destination IP address and port to that of the requester's. The requester's computer listens for a response (see figure 3.3) (Northrup,T. "Firewalls" http://www.microsoft.com/technet/security/topics/network/firewall.mspx.Microsoft Corp).

Another approach to understand how the TCP request is established between networks will be the *3-way handshake* connection. The concept behind this connection starts by ensuring that both sides are ready to transmit data, and that *both* ends know that the other end is ready *before* transmission actually starts. It allows both sides (requester and Server) to pick the initial sequence number to use (see figure 3.4). When opening a new connection, is easy to simply use an initial sequence number of 0. Thus, each side that wants to send data must be able to choose its initial sequence number.

The following is a step-by-step view of how the 3-way handshake works:

TCP ***X*** picks an initial sequence number (**X**_SEQ) and sends a segment to ***Z***

SYN_FLAG=1, ACK_FLAG=0, and SEQ=X_SEQ.

When TCP ***Z*** receives the SYN, it chooses its initial sequence number (**Z**_SEQ) and sends a TCP segment to ***X.***

ACK= (X_SEQ+1), ACK_BIT=1, SEQ=Z_SEQ, SYN_FLAG=1

When ***X*** receives ***Z***'s response, it acknowledges ***Z***'s choice of an initial sequence number by sending a dataless third segment.

SYN_FLAG=0, ACK=(Z_SEQ+1), ACK_BIT=1, SEQ=X_SEQ+1(data length = 0) … Data transfer may now begin.

Taken from Tanenbaum, A "Computer Networks" (p 496)

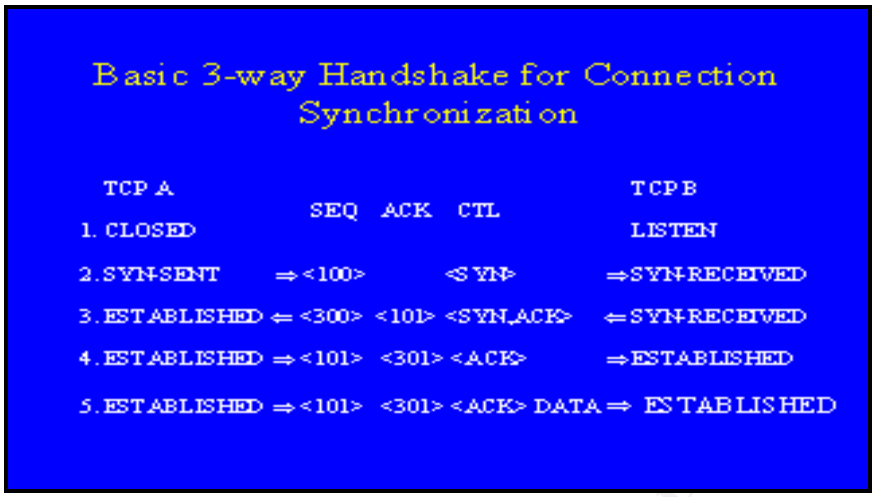


**Figure 3.3 Basic 3-way Handshake for Connection Synchronization**

# Section II. Risk Assessment

## 4. Impact Assessment

Impact assessments provide a detailed report on the current state of the system and the network's security level. This assessment helps to create a road map for correcting deficiencies. When evaluating a service or services, it's crucial not to make assumptions about things outside your control. For instance, when planning to connect a server on your private network, it is important not to assume that all the clients that connect to server are to be the ONLY for those clients in the internal network to prevent compromising the network. In the same way, if a station is running as a client in the outside, no assumptions should be made when the system connects and authenticate unless there are means of controlling them.

The following is a simple risk assessment, which should be enough to familiarize the system's administrator(s) with the main goals of any security plan: *Confidentiality, Data integrity***,** and *Availability of information***.**

An information assessment should be the first step into getting to know the type of information that needs to be protected and the type of security needed to protect it, as they relate to confidentiality, integrity and availability of information.

Following the assessment, security recommendations should be discussed and implemented prior to allow or deny users access to resources. This assessment should be used in conjunction with the departmental security checklist policies, which should contain steps for addressing the risks (if any), identified in during or after the assessment.

Security checklist:

1. Physical Security **-** Are the systems physically secured?
2. Passwords **-** Have appropriate passwords been enforced?
3. Virus Protection **-** Is the anti-virus software regularly updated?
4. Data Backup **-** Are the servers periodically backed up?
5. Operating Systems **-** Are the operating systems updated with current security patches?
6. Disaster Recovery **–** Is the disaster recovery plan current and updated?

## 4.1. Information Assessment

An effective risk management process is an important component of a successful IT security program. Security risk analysis, otherwise known as risk or impact assessment, is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed. The following impact assessments provide a method to identify the type of data and the type of protection needed to guard/secure the network assets as they relate to *privacy, reliability, and availability* of information (see sample below). Once the information is gathered, the data is assessed and analyzed using 2 essential approaches the quantitative and qualitative risk analysis methods (The Risk Analysis Directory "Introduction to Risk Analysis" http://www.security-risk-analysis.com/introduction.htm.)

**Quantitative Risk Analysis**

This approach employs two fundamental elements; the probability of an event occurring and the likely loss should it occur.

**Qualitative Risk Analysis**

Qualitative risk analysis (mostly use) methodology uses of 3 interrelated elements: Threats, Vulnerabilities and Controls (TVC)

1. **Threats** - Refers to the number of things that can go wrong in the event of a system 'attack.' If a systems or application is vulnerable to a threat, it is considered a risk.

2. **Vulnerabilities** - Refers to the number of things that can make a system more prone to attack by a threat or make an attack more likely to have some success or impact. If there's no vulnerability, regardless the threat, there is no risk.

3. **Controls** - Refers to the countermeasures for vulnerabilities

- *Deterrent* - reduce the likelihood of a deliberate attack
- *Preventative* - protect vulnerabilities and reduce the impact of an attack
- *Corrective* - reduce the effect of an attack
- *Detective* - discover attacks and trigger preventative or corrective controls

The following is use -*only*- as a sample of a security risk analysis.

***Privacy risk*** is the impact of unauthorized access to information assets, such as bookkeeping records, passwords, computer resources (hardware and software), confidential information, etc.

- If the data being accessed is classified as sensitive, or any other sensitive or confidential information, what is the probability that the confidentiality of the information could be compromised?

  **Probability**: High ____ Medium ____ Low ____
  **Impact**: High ____ Medium ____ Low ____

***Reliability risk*** addresses the impact of accessing inaccurate data to make business or management decisions. The disclosure of incorrect information could lead to a loss of business, and /or possible legal actions.

- If accessing sensitive information, or any type of confidential information, what is the probability that the data integrity could be compromised?

  **Probability**: High ____ Medium ____ Low ____
  **Impact**: High ____ Medium ____ Low ____

***Availability risk*** could be defined as the impact or activity that will result in due to failure and inoperative systems.

- If highly dependent upon accessing information, what is the probability of losing your access for long periods of time?

  **Probability**: High ____ Medium ____ Low ____
  **Impact**: High ____ Medium ____ Low ____

Each variable (privacy, reliability, and availability) must be assessed individually. Once the information is analyzed a risk assessment is performed and corrective action(s) should be taken to promote the protection and security of the information and resources.

| | Privacy – Reliability – Availability | Risk | |
|---|---|---|---|
| - | High Probability and High Impact | Results | Action |
| - | Medium Probability and High Impact | Results | Action |
| - | Low Probability and High Impact | Results | Action |
| - | High Probability and Medium Impact | Results | Action |
| - | Medium Probability and Medium Impact | Results | Action |
| - | Low Probability and Medium Impact | Results | Action |
| - | High Probability and Low Impact | Results | Action |
| - | Medium Probability and Low Impact | Results | Action |
| - | Low Probability and Low Impact | Results | Action |

# Section III. Systems Defense

## 5. Defense Overview

The Internet is open hole of new security or “vulnerabilities”. Some of these security risks are un-authorized access to systems, malicious attacks, viruses, worms, and identity theft (i.e. credit card fraud). When a request comes to the firewall a service is set with predefined rules that trigger a specific task, such as accept or deny traffic from or to a private network.

Firewalls are an essential part of a secure environment, security managers should be aware of the type of system’s attacks that can compromise their networks. The main idea of implementing security, i.e. a firewall, is to provide protecting services against possible attacks. In order to protect information, it is necessary to know what is being protected and what to protect them against (see section 4 - Impact Assessment).

## 5.1. System Attacks

So what exactly is a firewall protecting from? Well designed firewalls, should be able to safeguard networks from possible attacks that could compromise the integrity of information on private, public or personal systems. An attackers ("hacker" in today's jargon) have many ways of gaining access to private systems, as they explore system's vulnerabilities, and continuously exposing entire systems to malicious activities and attacks. Attacker's malicious activities are those activities that may result in damage of or unauthorized access to information by developing viruses, worms, and even identity theft.

The following section will outline and explain the most common types of attacks*: intrusion, denial of service (DoS), and information theft* (See Appendix A, table 5.1 most common attacks) as these forms of attacks could compromise entire network systems and their security.

### 5.1.1. Intrusion

As stated before, attackers have many ways to get access to computer systems. *Intrusions, social engineering, intelligence work, and traffic analyzer* or *eavesdropping* are among the most common type of computer attacks. The main idea of an *intrusion* is that the attacker tries to gain access to other user's computers and use them as if they were legitimate users. Some techniques used by attackers to gain access to system, such as *guesswork,* in which the attacker tries account names and passwords combinations until one works.

*Social engineering* attacks, is the kind of intrusion in which the attacker pretending to be the user in need, calls helpdesk and requests a password. Once the password is obtained, the attacker has access to systems and manipulates information without going to extensive processes.

*Intelligence work* (spying), the attacker goes through the user's personal belongings (notebooks, check books, correspondence, garbage cans, etc) in order to guess usernames and passwords.

Another type of intrusion is network *traffic analyzer* or *eavesdropping,* which consists in sniffing (captures data) credentials off the wire as users log in to a server, and then the attacker replays them to gain access.

### 5.1.2. Denial of Service

A *denial of service (DoS)* attack is one that's aimed entirely at preventing access to computers and/or resources. So the way attackers set a DoS is by flooding a system or network by sending (packets) requests. The system spends all its time and resources responding to these requests, creating a system lockup of “flood”.

Flooding is the simplest and most common way to carry out a DoS attack, an attack of this type is so powerful that it is capable of disabling services, reroute traffic or replace information (i.e. routing tables, ACLs, etc).

As a result of these types of attacks, one of the most important features of a security system, such as a firewall system, is to set up security measurement services so that if and when a port is flooded, the rest of the services stay up, preventing a partial or complete shut down.

### 5.1.3. Information Theft

*Information theft*, one of the fastest growing criminal activities now, this is a type of attack in which the attacker(s) do not need to have direct access to a system to gain access to confidential information; it does not need to be active or very technical. Frequently, this kind of attacks utilizes Internet services that are designed to give out information about individuals or other services like purchasing databases. Most attackers use the information gathered to gain access to systems, so they're generally looking for usernames and passwords (see IP spoofing definition). Once a username and password have been obtained, it becomes easier for the attacker to try to access, alter information, or even gain full control of the user(s)’ computers to maliciously managed entire networks.

IP Spoofing can yield access to user accounts and passwords, these attacks also can be used in other ways. A very common way attackers use to obtained information is by installing network sniffers. This technology allows any computer connected to a local area network to see all the traffic that passes across that LAN. Because traffic that crosses the Internet may cross any number of private networks, it is a tactic used by attackers to find out what systems are compromise gathering as much information as possible (Cisco Systems http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch2.htm).

# Section IV. Implementation

## 6. Firewall Implementation

Before implementing a firewall, it is important to have all the necessary pieces in place. Having an understanding about system security is a must. First, create a network diagram of the essential security requirements, before the actual firewall is implemented. Second, have an assessment of the information that will be protected. Finally, be aware of the type risks associated as a private network connects to the public network (Internet) in order to be able to protect the system(s) against them. For instance, malicious activities such as information and identity theft, virus, etc, that could compromise (see section 5) information system and its resources.

### 6.1. Diagram

A network diagram is an essential requirement in the planning stage. This diagram should illustrate, in a big scale, what the system will be accomplishing once it is implemented. It also will further help in the creation of the rules (see Figure 6.1) as well as access controls.

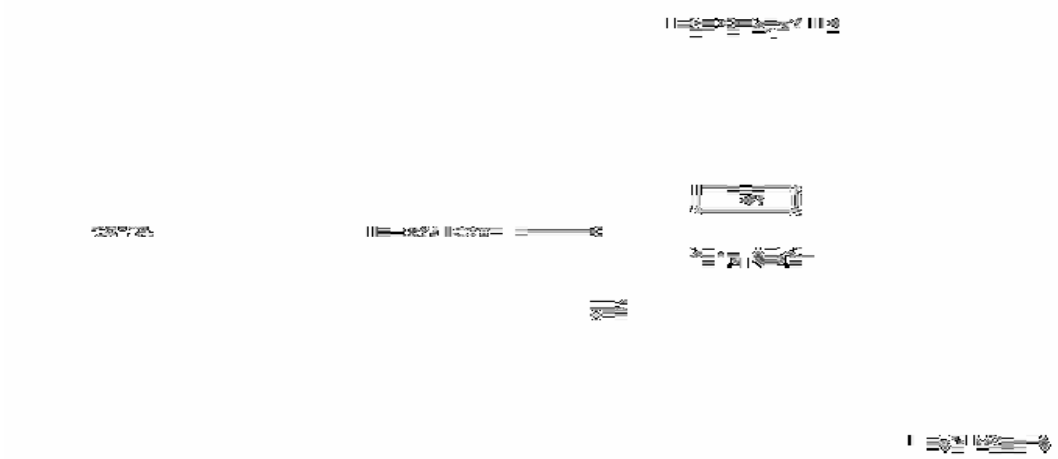

**Figure 6.1 Planning - Firewall Diagram**

## 6.2. Firewall Rules

Although, some firewalls have the ability to order the rules automatically (this can be a good and/or bad feature). All firewalls have rule sets. These rules tells the "firewall" system the type of traffic to let in and out (allow or deny) of the network. The rules on a firewall must be in a very specific order or they will not work properly (see Figure 6.2). Some basic rules in any firewall are: *Deny all inbound traffic* unless explicitly authorized (i.e. VPN users, network administrators, etc), and leave traffic open from internal users out. *Log all Deny* rules (to monitor unexpected system behaviors). Finally, *Deny* all inbound traffic with network addresses matching any of the internal's network addresses (Checkpoint "Managing Check Point FireWall-1." www.checkpoint.com).

The firewall rules filters the use of the TCP "well known ports" to permit, deny, or re-route access to particular Internet services. For instance many firewalls block all **inward** traffic except for email by rejecting all externally sourced packets bound for any port other than the SMTP (Simple Mail Transfer Protocol) port 25, or it can also route all HTML or Web traffic (port 80) to a particular host.


**Figure 6.2 Check Point – Firewall rule base**

## 6.3. NAT

NAT offers the ability to translate private IP addresses into public IP addresses and as a safety issue, it hides the internal topology of the private network(s).

There are four types of NAT configurations to be aware of: one-to-one, many-to-one, one-to-many, and many-to-many addressing.

On the one-to-one addressing NAT configuration, an internal IP address is mapped to a different external public IP address, usually the Firewall's external IP). For must private networks a simple one-to-one NAT capabilities are probably sufficient. The many-to-one addressing configuration means that multiple internal IP addresses (private IPs) can be mapped to one external – Public - IP address (see Figure 6.3). This process is done to hide the whole private network IP scope behind the firewall. The many-to-many NAT addressing is use for mapping groups of internal or external IP addresses with different groups of IP addresses on other networks. In a one-to-many NAT setting is commonly used in load-balancing scenarios, in which case one IP address is separated it in two. This is an advanced setting used by major communications providers (Elizabeth D. Zwicky E, Cooper S, & Chapman B. *"Building Internet Firewalls."*)

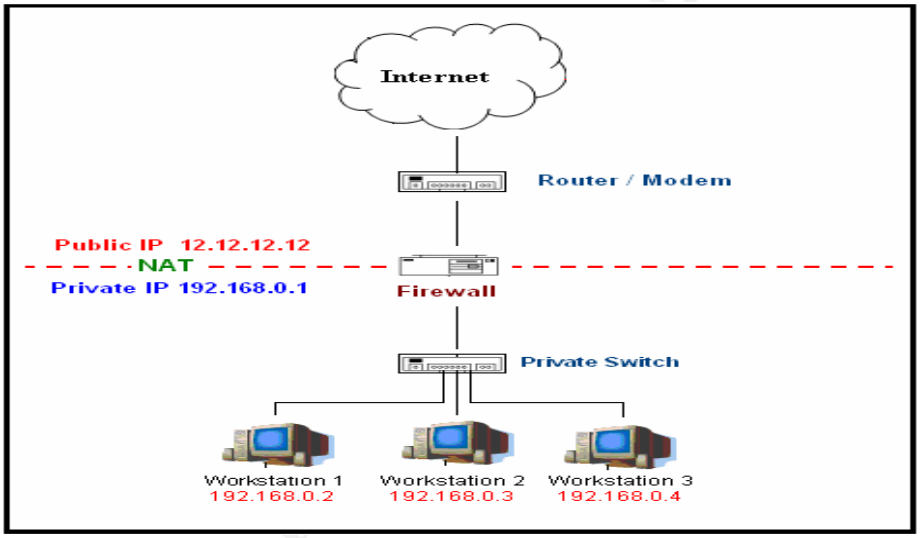


**Figure 6.3 Many-to-One NAT (Network Address Translation)**

## 6.4. Demilitarized Zone – DMZ

A DMZ (Demilitarized Zone) is an essential piece for securing a network. A DMZ provides a multilayer protection system between the Internet and the internal network of an organization. Demilitarized Zone -DMZ- is a term taken from military intelligence and is described as a safety zone between battle lines (i.e. the zone between North and South Korea). In the computer networking field, this refers to an area within the firewall, between the public network (Internet) and the internal network. This zone is **neither** in the internal network, nor is widely open to the Internet. Firewalls are configured to protect this zone with network traffic filtering capabilities.

In order to better protect the private network, it is recommended that a DMZ includes front-end servers, back-end servers, and a firewall. The firewalls protect the front-end servers from the public network and filter traffic between the corporate network and back-end servers. Thus, storing sensitive data outside the DMZ runs the risk, of opening the private network to malicious attacks.

## 7. Conclusion

How much security is needed to protect a network? This question is directly related to the type, the sensibility and the amount of data required to be secured. The main goal of implementing a firewall solution is to prevent systems to be compromised.

A properly configured firewall will reduce the risk attacks, as well as preventing the unauthorized manipulation of system's resources, and malicious attacks, both from inside and outside, resulting in damage, modification, lost, or disclosure of confidential information, and interruption of business. A firewall offers sophisticated features to assist security administrators detecting any unusual network behaviors that could compromise information integrity and help avoiding attacks before they even take place (i.e. activity logs, alert systems, email warnings, etc).

## References


1. NIST – National Institute of Standards and technology – "History of Computer Security." http://csrc.nist.gov/publications/history/. Retrieved May 6, 2004.

2. Tanenbaum, A. "*Computer Networks*" (4th Edition). Prentice - Hall 2003.

3. Checkpoint. "Managing Check Point FireWall-1." http://www.checkpoint.com/support/technical/online_ug/firewall-14.0/oltoc.htm. Retrieved May 7, 2004.

4. McClure, S., Scambray, J., Kurtz, G. "*Hacking Exposed*" (4th Edition). McGraw-Hill/Osborne 2003.

5. Cisco Systems. "Why you need a firewall." http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch2.htm. Retrieved May 3, 2004.

6. By Elizabeth D. Zwicky, Simon Cooper, & D. Brent Chapman. *"Building Internet Firewalls."* (2nd Edition). O'Reilly 2000.

7. Microsoft Corporation. "Firewalls" by Tony Northrup. http://www.microsoft.com/technet/security/topics/network/firewall.mspx. Retrieved May 2, 2004.

8. United States Department of Justice. http://www.cybercrime.gov/. Retrieved May 7, 2004.

9. Intranet Journal. "Firewall Shopping 101" by Laura Tylor. http://www.intranetjournal.com/articles/200202/se_02_13_02a.html. Retrieved May 7, 2004.

10. The Risk Analysis Directory "Introduction to Risk Analysis" http://www.security-risk-analysis.com/introduction.htm. Retrieved May 10, 2004.

11. By Elizabeth D. Zwicky, Simon Cooper, & D. Brent Chapman. *"Building Internet Firewalls."* (2nd Edition). O'Reilly 2000. Online Catalog http://www.oreilly.com/catalog/fire2/chapter/ch13.html. Retrieved May 11, 2004.

12. Pfleeger, C & Pfleeger, S. "*Security in Computing*". (3rd Edition). Prentice Hall 2003.

# Appendix

# A

| Attacks | Description | Firewall Settings |
|---|---|---|
| **Command-channel attacks** | Is one that directly attacks a particular service's server by sending it commands in the same way it regularly receives them (down its command channel). There are two basic types of command-channel attacks; an attack that exploit valid commands to do undesirable things, and attacks that send invalid commands and exploit server bugs in dealing with invalid input. | A firewall can protect against command-channel attacks by restricting the number of machines to which attackers can open command channels and by providing a secured server on those machines. In some cases, it can also filter out clearly dangerous commands (for instance, invalid commands or commands you have decided not to allow). |
| **Denial of service** | Is one that's aimed entirely at preventing access to computers and/or resources. So the way attackers set a DoS is by flooding a system or network by sending (packets) requests. The system spends all its time and resources responding to these requests, creating a system lockup of "flood". | Firewalls can help prevent denial of service attacks (DoS) by filtering out forged or malformed requests before they reach servers. In addition, they can sometimes provide assistance by limiting the resources available to an attacker. For instance, a firewall can limit the rate with which it sends traffic to a server, or control the balance of allowed traffic so that a single source cannot monopolize services. |
| **Data-driven attacks** | Is one that involves the data transferred by a protocol, instead of the server that implements it. Once again, there are two types of data-driven attacks; attacks that involve evil data, and attacks that compromise good data. Viruses transmitted in electronic mail messages are data-driven attacks that involve evil data. Attacks that steal credit card numbers in transit are data-driven attacks that compromise good data. | A firewall can't do much about data-driven attacks; the data has to be allowed through, or you won't actually be able to do anything. In some cases, it's possible to filter out bad data. For instance, you can run virus scanners over email and other file transfer protocols. Your best bet, however, is to educate users to the risks they run when they bring files to their machine and when they send data out, and to provide appropriate tools allowing them to protect their computers and data. These include virus checkers and encryption software. |
| **Third-party attacks** | A third-party attack is one that doesn't involve the service you're intending to support at all but that uses the provisions you've made to support one service in order to attack a completely different one. For instance, if you allow inbound TCP connections to any port above 1024 in order to support some protocol, you are opening up a large number of opportunities for third-party attacks as people make inbound connections to completely different servers. | Third-party attacks can sometimes be prevented by the same sort of tactics used against command-channel attacks: limit the hosts that are accessible to ones where you know only the desired services are available, and/or do protocol checking to make certain that the commands you're getting are for the service you're trying to allow. |
| **False authentication of clients** | The subversion of the authentication that you require of your users, so that an attacker can successfully masquerade as one of your users. This risk is increased by some special properties of passwords. | A firewall cannot prevent false authentication of clients. It can, however, limit incoming connections to ones on which you enforce the use of nonreusable passwords |
| **Hijacking** | Allows an attacker to take over an open terminal or login session from a user who has been authenticated and authorized by the system. Hijacking attacks generally take place on a remote computer, although it is sometimes possible to hijack a connection from a computer on the route between the remote computer and your local computer | A firewall can rarely do anything about hijacking. Using a virtual private network with encryption will prevent it; so will protocols that use encryption with a shared secret between the client and the server, which will keep the hijacker from being able to send valid packets. Using TCP implementations that have highly unpredictable sequence numbers will decrease the possibility of hijacking TCP connections. It will not protect you from a hijacker that can see the legitimate traffic. Even somewhat unpredictable sequence numbers will help; hijacking attempts will create a burst of invalid packets that may be detectable by a firewall or an intrusion detection system. |
| **Packet sniffing** | Attackers may not need to hijack a connection in order to get the information you want to keep secret. By simply watching packets pass -- anywhere between the remote site and your site -- they can see any unencrypted information that is being transferred. *Packet sniffing* programs automate this watching of packets. | A firewall cannot do anything to prevent packet sniffing. Virtual private networks and encrypted protocols will not prevent packet sniffing, but they will make it less damaging. |
| **Replay** | An attacker who can't take over a connection or change a connection may still be able to do damage simply by saving up information that has gone past and sending it again. We've already discussed one variation of this attack, involving passwords. There are two kinds of *replays*, ones in which you have to be able to identify certain pieces of information (for instance, the password attacks), and ones where you simply resend the entire packet. | Once again, a firewall can do very little about replay attacks. In a few cases, where there is literally a replay of exactly the same packet, a stateful packet filter may be able to detect the duplication; however, in many cases, it's perfectly reasonable for that to happen. The primary protection against replay attacks is using a protocol that's not vulnerable to them (one that involves message integrity and includes a timestamp, for instance). |

**Table 5.1 Most Common Attacks**

All data was retrieved from *"Building Internet Firewalls."* (2nd Edition). O'Reilly 2000. Online Catalog http://www.oreilly.com/catalog/fire2/chapter/ch13.html.

Last Updated: July 25th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| Community SANS Omaha SEC401* | Omaha, NE | Aug 14, 2017 - Aug 19, 2017 | Community SANS |
| SANS New York City 2017 | New York City, NY | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Salt Lake City 2017 | Salt Lake City, UT | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| SANS Adelaide 2017 | Adelaide, Australia | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style | Virginia Beach, VA | Aug 21, 2017 - Aug 26, 2017 | vLive |
| SANS Chicago 2017 | Chicago, IL | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| Community SANS Pasadena SEC401 @ NASA | Pasadena, CA | Aug 23, 2017 - Aug 30, 2017 | Community SANS |
| Mentor Session - SEC401 | Minneapolis, MN | Aug 29, 2017 - Oct 10, 2017 | Mentor |
| SANS San Francisco Fall 2017 | San Francisco, CA | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS Tampa - Clearwater 2017 | Clearwater, FL | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| Mentor Session - SEC401 | Edmonton, AB | Sep 06, 2017 - Oct 18, 2017 | Mentor |
| SANS Network Security 2017 | Las Vegas, NV | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| Community SANS Albany SEC401 | Albany, NY | Sep 11, 2017 - Sep 16, 2017 | Community SANS |
| Mentor Session - SEC401 | Ventura, CA | Sep 11, 2017 - Oct 12, 2017 | Mentor |
| Community SANS Columbia SEC401 | Columbia, MD | Sep 18, 2017 - Sep 23, 2017 | Community SANS |
| Community SANS Dallas SEC401 | Dallas, TX | Sep 18, 2017 - Sep 23, 2017 | Community SANS |
| Community SANS Boise SEC401 | Boise, ID | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | vLive |
| Community SANS New York SEC401 | New York, NY | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| Rocky Mountain Fall 2017 | Denver, CO | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS London September 2017 | London, United Kingdom | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Baltimore Fall 2017 | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Copenhagen 2017 | Copenhagen, Denmark | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Community SANS Sacramento SEC401 | Sacramento, CA | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| SANS DFIR Prague 2017 | Prague, Czech Republic | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| Mentor Session - SEC401 | Arlington, VA | Oct 04, 2017 - Nov 15, 2017 | Mentor |
| Community SANS Indianapolis SEC401 | Indianapolis, IN | Oct 09, 2017 - Oct 14, 2017 | Community SANS |