PRIME MINISTER'S OFFICE

NATIONAL AGENCY FOR CYBER SECURITY (ALCIRT)

REGULATION ON FIREWALL MANAGMENT

Approved with Order no.10 of 25.04.2016
Director of National Agency for
Cyber Security(AlCIRT)

April, 2016

TABLE OF CONTENT

Definitions 4
Summary 7
1.Introduction 9
1.1 Purpose 9
1.2 Scope of application 9
1.3 Structure of the document 9
2. Overview of Firewall Technologies 10
2.1 Firewall technologies 11
2.1.1 Packet Filtering 11
2.1.2 Stateful Inspection 13
2.1.3 Application Firewalls 14
2.1.4 Application-Proxy Gateway 15
2.1.5 Dedicated Proxy Servers 16
2.1.6 Virtual Private Network (VPN) 17
2.1.7 Network Access Control (Network Access Control) 17
2.1.8 Unified Threat Management (UTM) 18
2.1.9 Web application firewalls 18
2.1.10 Firewalls for Virtual Infrastructures 18
2.2 Firewall Inspection Restrictions 19
2.3 Summary of the Rules 19
3. Firewalls and Network Architecture 19
3.1 Network Models with Firewalls 20
3.2 Firewalls that act as Network Address Translators 22
3.3 Multilayer firewalls architecture 22
3.4 Summary of the Rules 23
4. Firewall Policies 23
4.1 Policies based on IP addresses and protocols 23
4.1.1 IP Addresses and Other IP characteristics 24
4.1.2 IPv6 25
4.1.3 TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) 25
4.1.4 ICMP (Internet Control Message Protocol) Basic Internet Protocol used for the exchange of error messages 25
4.1.5 IPsec protocols 26

4.2 Application-Based Policies **26**
4.3 User Based Identity Policies **27**
4.4 Policies based on network activity **27**
4.5 Summary of the Rules **28**
5. Planning and Implementing Firewalls **28**
5.1 The plan **29**
5.2 Configuration **31**
5.2.1 Hardware and software installation **32**
5.2.2 Policy Configuration **32**
5.2.3 Configuring logs and alarms **33**
5.3 Testing **33**
5.4 Installation **34**
5.5 Administration **35**

Definitions

- *Wireless* - Wireless (wireless) communication.
- *Log* - Consider any digital note on a particular event or activity.
- *Malware* - A dangerous software, which aims to stop operating a computer system , collects unauthorized information or taking control of a computer system.
- *Antivirus / Antispyware / Antimalware* - Programs that enable control, identifies, eliminate malicious software installed on computers (virus, trojan etc.)
- *Firewall* - Devices or a software program that is configured to control traffic passing through the network, allowing or blocking it based on a group of rules.
- *Intrusion Detection technology* - Inspection technology that analyzes protocols on application layer to compare manufacturer activity profile with observed events profiles to identify deviations.
- *Computer Incident* - an event occurring on a computer and compromising its confidentiality, integrity or availability of a computer or system; or of the data he holds
- Storage - Computer memory used for mass storage of data
- *Software* – Computer Progamms
- *VPN* - Virtual private networks that provide high security
- *Application-Proxy Gateway* - the quality of advanced firewalls combining control of access to the lowest layer with the highest layer functionality.
- *Proxies* - Applications that facilitate Internet access
- *Routers* - Network devices that manage and deliver network packets
- *Switches* - Network devices that send network packets

- *Username* - user name, string of characters that uniquely identifies one user in a computer system or network.

- *Password* - password, secret code of a user that should not be recognized by the other users , when is used with UserID, allows access to a system.

- *IDPS* - Cyber Attack Prevention Systems that monitor networks or computer systems.

- *Network* - Computer Network.

- *TLS* - A cryptographic protocol that provides security for data transfer over the Internet.

- *IP* - An electronic address consisting of a number of 32 bits.

- *UDP* - Network protocol used in cases where no reliable transfer is needed reliable.

- *FTP* - Technology that allows the transfer of files over the Internet.

- *Worm* - Malware which replicates itself in as many computer systems as possible.

- *SMNP* - Standard Internet Protocol for IP Network Device Management.

- *Encapsulation* - The process of packing data of the previous level and the addition of actual level data during the packet process.

- *Host* - The main computer or controller that provides computer services , or computers, or terminals connected through the network.

- *HTTP* - Application Protocol for Distributed Systems.

- *ICMP* - The basic Internet protocol used mainly for the exchange of error messages.

- *Port Span* - The process of copying network traffic to another gateway for monitoring purposes.

- *DHCP* - Network protocol that manages networked devices.

- *Tunning* - Configuration process for performance enhancement.

- *Spoofed* - Imitation of the address in order to look like someone else.

- *DNS* - Internet service that translates domain names into IP addresses.

- *Active X* - The technology community used for disseminating information.

- *Handshak*e - The process of commencing communication between two devices.

- *Payload* - Content of the network packet.

- *Debugging* - The process of finding errors.

- *Cashing* - Switching to the memory part which has very high communication speeds.

- *Scalability* - Ability to adjust to future quantitative increases.

- *Stateful firewall* - any firewall that performs stateful packet inspection is one firewall that keeps track of the state of the network connections. The firewall is programmed to distinguish legitimate packets that come from different types of links. Only the packets that match a known connection state will be allowed by the firewall. Others will be rejected.

- *Stateless firewall* - a firewall that handles each package individually. This firewall does not
  know if the package is part of an existing communication, new communication being created, or it's just a bad package

Summary

Firewalls are devices or programs that control the way the network traffic passes, between the network and the host, which may have different security status. Once, firewalls were distributed throughout the network's perimeter. This made it possible to equip with internal safeguards, but there was no recognition of all instances and forms of attacks and attacks that are sent from one host to another, who often do not pass on network firewalls. For this reason and for other factors, network designers often include functional firewalls in other countries outside the network perimeter to provide a higher level of security and to protect mobile devices, which are located on the external network.

Threats have gradually shifted from being the most widespread in the low-traffic layer layer to the application layer, which has reduced the overall firewall effectiveness in stopping threats that go into the communications network. However, firewalls still have to block threats that continue to be in the network traffic layer. Firewalls can also provide protection in the application layer, by complementing the capabilities of network security technologies.

There are several types of firewalls that range from network traffic analysis and the permission, or blocking, of specific instances by comparing the traffic characteristics with the existing policies. Understanding the capabilities of each type of firewall, and designing policies for firewalls and the acquisition of a firewall technology to effectively address the needs of institutions, are critical to achieving network traffic protection. This regulation gives a general overview of firewall technologies, discusses their security capabilities, advantages and disadvantages in detail. Also, this document gives examples of where firewalls can be placed on the network and the implications of placing firewalls on specific locations. This document provides recommendations for creating firewall policies and for selecting, configuring, testing, distributing, and managing firewall solutions.

The regulation does not cover technologies called “Firewall”, but mainly examines only activities in the application layer, not in the low level of network traffic. Technologies that are focused on activities of particular types of applications, such as firewalls that block suspicious emails, are not covered in detail in this document.

To improve the effectiveness and security of firewalls, institutions should implement the following recommendations:

Creating a firewall policy that specifies how incoming and outgoing traffic should be handled.

The firewall policy defines how the institution's firewall should handle incoming and outgoing network traffic for a specific IP address, and the rank of addresses, protocols, applications, and content types based on the institution's security policy information.

Institutions should carry out a risk analysis to establish a list of the type of traffic the institution needs and how should be provided this traffic - including traffic types that can traverse the firewall in special circumstances. Examples of policy requirements are : allowing only IP (Internet Protocol) protocols to pass, using the source and destination IP, the designated Transmission Control Protocol (TCP) protocol, and access to UDP (User Datagram Protocol) ports, the Internet Control Message Protocol (ICMP) types and the codes to be used. Inbound and outbound traffic that is not allowed by firewall policy should be blocked, because this traffic does not need the institution.This practice reduces the risk of attacks and can also reduce traffic to the network of the institution.

Identify all the requirements to be considered, when determining the firewalls to be implemented.

Institutions should consider some elements in the selection and planning of firewalls. They should determine which network spaces should be protected, and which types of firewalle technology will be more effective for the types of traffic that require protection. It should also be considered the importance of performance, for integrating firewalls into existing network and security infrastructure. Designing firewall solutions involves requirements related to the physical environment and personnel, as well as considerations for future requests, such as the adoption of new IPv6 technologies or virtual private networks (VPNs).

Creating a community of rules ,which are implemented by firewall policies while retaining its performance.

Firewall rules group should be as specific about the network traffic they control. Creating a set of rules includes determining the types of traffic that are required, including protocols that the firewall might need for management purposes. Details of creating a rule community vary from the type of firewall and from specific products,but many firewalls can improve their performance by optimizing the community of their rules.

Management of the architecture of firewalls, policies, programs and other components throughout the life of the firewall.

There are many aspects of firewall management. For example, choosing the type or types of firewalls to implement and their position within the network, can significantly affect security policies that the firewall can enforce. Components of firewall performance should be monitored to identify and address potential resource issues. Logs and alerts should be constantly monitored to identify threats - successful and unsuccessful ones. The rules of firewalls and

policies, should be managed by controlled processes due to the impact on security and business operations.Firewalls should be periodically updated to avoid vulnerabilities.

1.Introduction

The National Computer Security Agency (ALCIRT) based on Decision no. 766 dated 14.09.2011, as amended, pursuant to point 3 letter d).
"Issues network security rules and state computer systems".

1.1 Purpose

This regulation aims to help institutions understand the need for efficient management of firewall technologies and firewall policies. It provides practical guidelines for policy development and selection, configuration, testing, implementation and firewall management

1.2 Scope of application

This regulation was first created for the technical staff of information technology, such as network personnel, security and system managers and administrators, who are responsible for designing firewalls, selecting, implementing and managing them.The content of the regulation assumes possessing basic network knowledge and network security.

1.3 Structure of the document

The regulation is organized in four chapters:

- The second chapter presents some firewall technology including filtering of packages, packet inspection, proxy gateway application, and also provides information on host-based personal firewalls.

- The third chapter presents the installation of firewalls in the network architecture.

- The fourth chapter presents firewall policies and gives recommendations on types of traffic that are termed as prohibited.

- Chapter five presents an overview of the planning and implementation of firewalls.This section lists the factors that should be considered for selecting firewalls, and provides recommendations for firewall configuration, testing, implementation, and management.

2. Overview of Firewall Technologies

Firewalls are devices or programs that control the way the network traffic flows between the network and the host, which may have different security status, While firewalls are often discussed in Internet connection contexts, they can also be implemented in other network environments. For example, many institutional networks implement firewalls, to limit the connections to the internal network and from the internal network to the external network. By implementing firewalls to control the network, institutions can prevent unauthorized access to its resources and systems.
Including a firewall provides an additional layer of security.

There are several types of firewall technologies. One way to compare compatibility is to look at each TCP / IP layer. TCP / IP communications consist of four layers that work together to transfer data between hosts. When a user wants to transfer data to the network, the data pass from the highest layer through the middle layer to the lower layer, adding information to each of them. The lower layer sends the data collected on the physical network, then sends them to the highest layers to the destination. In other words, the data produced by one layer is encapsulated in a larger unit in the underlay layer.

Application layer. This layer sends and receives data for certain applications, such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).The application layer has the protocol layer inside it. For example, SMTP encapsulates the RFC (Request for Comments), which encapsulates Multipurpose Internet Mail Extensions (MIME), which encapsulates other formats such as Hypertext Markup Language (HTML).
Transport layer. This layer provides connectivity for service delivery across the application layer between networks, and can provide the reliability of communication. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are the most frequently used protocols in the transport layer
IP layer (also known as network layer). This layer routinizes packets in the network. Internet Protocol Version 4 (IPv4), is the main layer network protocol. Other protocols used in this layer are IPv6, ICMP and IGMP.
Hardware layer (also known as Layer Data Link). This layer addresses communications in physical layer communications. The most familiar protocol of this layer is Ethernet.

Addresses in the Data Link, which are assigned to the network interface are referred to as *media access control* (MAC) addresses - an example of this is an EtherNet address that belongs to an EtherNet card. Firewall policies rarely relate to the layer of data. The addresses in the network layer are referred to as IP addresses. The transport layer identifies specific network applications and communication sessions; a host can have an indefinite number of session layers of transport with other hosts on the same network. The transport layer can also include the notion of the gate - the port number of the destination, generally identifies a host service on the hosting host, and the source gateway generally identifies the port number at the source host where the destination host should respond.

Transport protocols like TCP and UDP have ports, while other transport protocols do not have. The source gateway combination with the IP address of the source and the destination IP address with the destination port assist in determining the session. The top layer represents end user applications - firewalls can inspect application traffic and can use them as the basis for policy decisions.

Basic firewalls can operate in one or more layers - usually in the lower layers - while most advanced firewalls operate in all layers. The latter can perform a more detailed and more regular examination.

2.1 Firewall technologies

This section of the regulation provides a general overview of firewall technologies and basic information on the capabilities of the most commonly used types. The implementation process of the firewall is combined with different technology especially with routing and other technology that are often associated with firewalls but are part of these types of technologies.
For example: NAT (Network Address Translation) is considered to be firewall technology but actually is routing technology. Many firewalls include filter character elements to enforce institution policies that are not directly related to security.Some firewalls also include Intrusion Prevention System (IPS) technologies, which can react to the attacks they detect to prevent damage to systems that are protected with firewall.
Firewalls are placed on the perimeter of the network. These kind of firewalls can have an external and internal interface, where the external interface is the only one located in the external network. These two interfaces are often refe, is inadequate because firewall policies work in both directions; for example, there may be a policy that stops executing an executable code to be sent from within the perimeter outside it.

2.1.1 Packet Filtering

The main feature of a firewall is packet filtering. Older firewalls that were just packet filters were basically routines that provided access control features for host addresses and communication sessions. These devices also known as stateless inspection firewalls (see definition: stateless inspection firewalls) does not leave trace at the traffic flow situation that

passes through the firewall, which means, for example: that they can not associate multiple requests within a single session to others.
Packet filtering is inside of modern firewalls, but there are some firewalls that are sold today that make only statelesspacket filtering (see definitions). Unlike most advanced filters, packet filters do not focus on package contents. Their access control functionality is managed by a set of directives that we refer to as a set of rules. Packet filtering capabilities are built on most operating systems and devices that are capable of routing. The most common example of a clean package filtering device is a router-network that implements the access control list. Firewalls in their most common form operate on the network layer. This provides network access control based on some specific pieces of information contained in the packages, including:

- Source IP Address IP address --- the host address from which the package originates (such as:192.168.1.1)
- Destination packet IP address --- host address where packets are trying to reach (such as:192.168.2.1)
- The network or transport protocol that is used for communication between the host of source and destination as: TCP, UDP or ICMP.
- Some features of transport layer communication sessions, such as the source port and destination session.
- Interfaces covered by their packets and directions (incoming and outgoing).

Inbound traffic filtering is also known as input filtering. Even outgoing traffic can be filtered, and the process is known as outbound filtering. Institutions may apply restrictions on their incoming, outbound traffic such as blocking the use of File Transfer Protocol (FTP) or preventing Denial of Service attacks initiated by the institution against external entities. Institutions should only allow that outbound traffic that uses source IP addresses from institutions - a process that helps block spoofed addresses traffic in other networks. False addresses can be caused by malicious such as infestations from malware infections or compromised hosts that are used to attack or unintentional misconfiguration.

Stateless packet filters are generally more vulnerable to attacks that use problems within TCP / IP protocol specifications. For example: many packet filters are unable to detect when the address information in the network layer of a packet has been fake or edited. Spoofing attacks, such as the use of fake addresses on packet heads, are commonly used to avoid security controls on firewall platforms. Firewalls operating in high layers can hamper spoofing attacks by verifying that the communication session is created, or authenticating users before allowing the exchange of information. For this reason, many firewalls using packet filters maintain the status of packet information that passes through the firewall.
Some package filters can filter packages that are fragmented. Packet fragmentation is allowed by TCP / IP specification. However fragment packets are used to make the attacks difficult to detect (placing them inside the packages fragmented), and fragmentation itself is used as a form of attack. For example: some network-based attacks have used packages that should not exist in normal communications,as sending packages fragments, but not the first fragment, or sending packages fragments which overlap each other. To prevent the use of fragmented packets in attacks, some firewalls are configured to block fragmented packets.

Today, fragmented Internet packets often occur not because of attacks but because of virtual private networking technologies (VPNs) that encapsulate the packets within the other packets. If packet encapsulation can cause overrun of the maximum size of the broadcast medium, one of the packets should be fragmented. Blocking fragmented packets from firewalls is a common phenomenon of virtual private network (VPN) interaction.

Some firewalls can reassemble the fragments before they pass them over to the network internal, however this requires additional firewall resources, especially memory. Firewalls that have reassembly quality should be carefully implemented, otherwise they can be attacked with DDoS. Choosing the implementation of blocking, reassembling, or switching of fragmented packets is set by the interaction between the network and the system as a whole. In this way, the automatic blocking of all fragmented packages is not recommended because of the need to use fragmentation over the Internet.

2.1.2 Stateful Inspection

Stateful inspection improves the functionality of packet filtering by following the status of connections and blocking packets that deviate from the state of the set. As in packet filtering, stateful inspection monitors packets in the network layer and inspects them to see if they match existing firewall rules or unlike filtering the stateful inspection packages keeping track of each connection in a table state table. While the status table details range from the type of firewall, they generally include the source IP address, the destination IP address, the port numbers, and the status information of the connection.

There are three main conditions for TCP traffic - establishing connectivity, usage, and termination (which refers to the end of a late communications request and the status of a connection that is inactive for a long time). Stateful firewall inspection examines certain values in TCP heads for monitoring each state.
Each new packet is compared to the firewall's firewall table to determine whether the condition of the package matches its expected state. For example, an attack can generate a packet with a head which indicates that it is part of an existing communication in the hope that it will pass through the firewall. If the firewall uses stateful inspection, it first verifies that the package is part of an existing communication in the status table.

In the simplest case, a firewall will allow the passage of packages that appear to be part of existing communications (or a communication that is not fully created). However, many firewalls know the car's status for protocols like TCP and UDP, and they can block packets that do not exactly match the proper car situation. For example, usually firewalls control attributes as sequences of TCP numbers and reject packets that are out of this sequence. When the firewall also provides the NAT (Network Address Translator) service, it often includes information about NAT in its table of situation.

Table 2-1 gives an example of a state table. If a device on the internal network (for example 192.168.1.100) attempts to connect to a non-firewall device (192.0.2.71), the connection

attempt at the beginning is checked to see if it is allowed by the firewall rule set. If yes, in the status table is added a new line that indicates the creation of a new session, as shown in Table 2-1 in the first line in "Connection Status". If 192.0.2.71 and 192.168.1.100 end TCP handshake, connection status will change from "Initiated" to"Created" and traffic matching this connection line will be allowed to pass from the firewall.

Table 2-1 Example of a status table

Source Address	Source Port	Destination Adress	Destination port	Connection status
192.168.1.100	1030	192.0.2.71	80	initiated
192.168.1.102	1031	10.12.18.74	80	created
192.168.1.101	1033	10.66.32.122	25	created
192.168.1.105	1035	10.231.32.12	79	created

Because some protocols, such as UDP, are connectless and do not have a formal process for initiating, creating, and terminating a communications link, their status can not be determined in the transport layer as in the case of TCP. For these protocols, most firewalls with stateful inspection can only track the source and destination IP addresses and ports. UDP packages must match a row from the status table based on the above elements - a DNS response from external sources will only be allowed if the firewall has previously detected a DNS query from an internal source. Because the firewall is unable to determine when a communication session is completed, the line is removed from the status table after a pre-configured value has been reached. Communication level firewalls can recognize DNS over UDP that will end the session after receiving the DNS response. Likewise, it can work with the Network Time Protocol (NTP) protocol.

2.1.3 Application Firewalls

A new element in stateful inspection is the addition of capabilities in stateful protocol analysis, which some manufacturers refer to as deep packet inspection. Stateful protocol analysis improves stateful inspection standards by adding basic intrusion detection technology. This causes a firewall to allow or deny access based on how an application runs on the network. For example, an application firewall can determine whether the email contains attachment types that the institution does not allow as an executable file.exe. Another feature is that the firewall can block the connections over which specific actions are being performed. This feature can also be used to allow or deny Web pages that contain specific types of content such as Java or ActiveX or those that have Secure Sockets Layer (SSL) certificates that have been signed by a specific CA (Certification Authority) .Firewall applications can make it possible to identify unexpected command sequences such as the use of the same command repeatedly or the use of a command that is not preceded by another command from which it is hanged. These suspicious commands often originate from buffer overflow attacks, DoS attacks, malicious software, and other types of attacks that occur within protocol applications such as Hypertext Transfer Protocol (HTTP).

Another attribute is the validity of individual input commands, the minimum and maximum length of arguments. For example, the argument of a 1000-character username is doubtful. Application firewalls are implemented for HTTP protocols, SMTP (Post Office Protocol) and Internet Message Access Protocol (IMAP), Voice over IP (VoIP), and Extensible Markup Language (XML). Firewalls that have the capabilities of stateful inspection and stateful protocol analysis capabilities together can not do more detection and attack prevention than IDPS systems.

2.1.4 Application-Proxy Gateway

These firewalls contain a proxy agent acting as an intermediary between two hosts wishing to communicate with each other, and never allowing direct connection between them. Every successful link attempt actually results in the creation of two separate connections - one between the client and the proxy server, and the other between the proxy server and the real destination. Because external hosts only communicate with a proxy agent, the internal IP addresses are not visible to the external network. The proxy agent interacts directly with the firewall community to determine if a concrete network instance is allowed to pass through the firewall.

In addition to the firewall rules community, some proxy agents have the power to request authentication for each individual network user. This authentication can take some forms, including user ID and password, biometric elements,etc.

Just like firewall applications, and proxy gateways operate on the application layer and can inspect the current traffic content. These gateways can also perform TCP handshake with the source system and are able to protect against exploitation in any communication sequence. In addition, ports can make decisions to allow or allow traffic based on the application application or payload header. Once the gateway determines that the data is allowed, they are sent to the destination host.

Application-proxy gateways change application firewalls. First, an application-proxy gateway can provide a higher level of security for some applications because it hampers direct links between two hosts and inspects traffic content to identify policy violations. Another important advantage is that some application-proxy gateways have the ability to decrypt packages, to examine them, and to encrypt them before sending them to the destination host. When choosing the type of firewall to be implemented, it is important to decide if the firewall should actually act as an application proxy in order to comply with the special policies required by the institution.

Application-proxy gateway firewalls can also have disadvantages when compared to packet filtering and stateful inspection. First, due to the detailed inspection of the packets, the firewall spends more time reading and interpreting each packet. Because of these, these gateways are not suitable for high bandwidth applications or real-time applications, but there are also high-bandwidth application-proxy gateways. To reduce the load on the firewall, to provide non-sensitive services such as e-mail and web traffic, a dedicated proxy server can be used. Another disadvantage is that the application-proxy gateway tends to be limited in terms of support for new network protocols and applications. Many application-proxy gateways manufacturers provide general proxy agents to support protocols or unspecified network applications. These

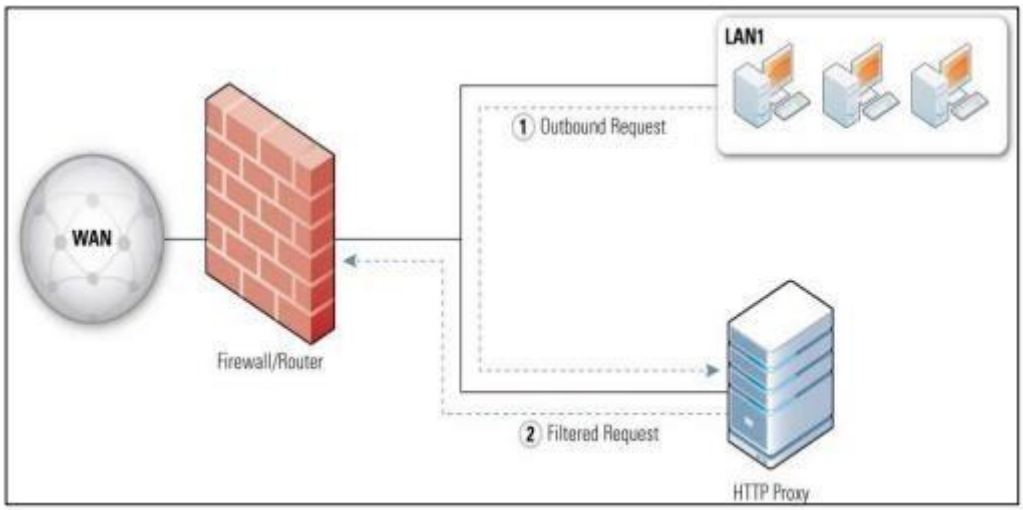
general agents tend to deny many of the application-proxy gateway architecture's strengths because they simply allow traffic to pass through the firewall.

2.1.5 Dedicated Proxy Servers

Dedicated proxy servers differ from application-proxy gateways because they usually have more limited firewalling capabilities. Many dedicated proxy servers are specific to applications, and some perform protocol analysis and validation like HTTP. Because these servers have limited firewalling capabilities, such as traffic jam based on their source or destination, they are typically implemented on traditional platforms of firewalls. Usually, a main firewall can accept incoming traffic, determine which application is targeted, and direct traffic to the appropriate proxy server (for example, proxy email). This server must perform filtering or logon traffic, and then forward it to the interior system. A proxy server can accept outbound traffic directly from the internal system, filter it or traverse it and pass it over to the firewall to send it out. A typical example is the HTTP proxy, implemented after the firewall - users who want to connect to this proxy must connect through external web services. Dedicated proxy servers are generally used to lower the load of firewalls and perform specialized filtering that can be difficult to accomplish by the firewall.

In recent years, the use of proxy servers for incoming traffic has been drastically reduced. This is because a proxy server for incoming traffic has to imitate the capabilities of the real server being protected, which makes it almost impossible when it comes to save a server with many features. In addition, the main features that the proxy servers for incoming traffic (login, access control) must have are usually built into real-time servers. Many proxy servers in use are proxy servers for outbound traffic, and are usually HTTP proxies.

The following figure shows a simple network diagram that implements a dedicated HTTP proxy server, which is deployed after another firewall system. HTTP proxy will handle outbound connections to external web servers and filter active content. User requests initially go to the proxy, and the proxy then sends the requests to the external web server. The response from that web server then returns to the proxy, which conveys it to the user.



2.1.6 Virtual Private Network (VPN)

Firewall devices are sometimes required to do more than just blocking unwanted traffic. A common requirement for these firewalls is to encrypt and decrypt the specific network traffic that flows between the protected and external networks. This almost always includes the virtual private network (VPN), which use additional protocols to encrypt traffic and provide user authentication and integrity control. VPNs are often used to provide secure network communication over unsafe networks. for
For example, VPN technology is widely usable to extend the protected network to a large institution over the Internet, and often to provide remote control over the internal network of the institution via the Internet.

The two usual choices to secure VPNs are IPsec and SSL / TLS (Secure Sockets Layer / Transport Layer Security). The two most common virtual private network (VPN) architectures are gateway-to-gateway and host-to-gateway. Gateway-to-gateway architecture links sites through the use of virtual private network (VPN) ports, a case similar to the affiliation of an institution with the head office. A virtual private network (VPN) gateway is usually part of another network device such as a firewall or router. The second-tier architecture, the host to gateway, provides a secure network connection, commonly called remote users, and is deployed outside the facility. In this case, the user creates a secure connection to the institution gateway. For VPN gateway-to-gateway and host-to-gateway, VPN functionality is often part of the firewall itself. Setting it up after the firewall requires VPN traffic to pass through the firewall while encryption occurs, preventing traffic inspections from the firewall.

All host-to-gateway VPN allows the firewall administrator to decide which of the users will have access to certain network resources. This access control is usually available for user groups or individual users. This means that VPN policies determine which users or groups are authorized to access the resources. VPNs typically work with authentication protocols such as Remote Authentication Dial In User Service (RADIUS). RADIUS uses some credential types for authentication, such as username and password, digital signature and device hardware (hardware tokens). Another protocol commonly used by VPN is the Lightweight Directory Access Protocol (LDAP), which is especially useful for determining access to individual users and groups.
To enable VPN functionality on a firewall requires additional resources that depend on the amount of traffic that flows through the VPN and the type of encryption that is being used. For some environments, additional VPN-related traffic may require additional capacity and resource planning. Planning is also needed to determine the type of VPN (gateway-togateway and / or host-to-gateway) that should be included in the firewall.

2.1.7 Network Access Control (Network Access Control)

Another firewall request on the network boundary is to run user controls for remote access user connections and allow or allow access based on these controls. This control, usually called network access control (NAC) or network access protection (NAP), allows access based on

user credentials and the results performed by the control performed on the computers used. This check usually consists of the following elements of the institution's policies:
- Latest updates against malware and firewall software
- Configuration rules for antimalware and firewall software
- The time since last scanning for malware
- The level of patches for the operating system and selected applications
- Configuration of security for the operating system and selected applications

If user credentials are acceptable, but the device itself does not pass the control successfully, the user and the device may receive limited access to the internal network.

2.1.8 Unified Threat Management (UTM)

Many firewalls combine multiple features into a single system, the idea is that it is easier to set up and maintain policy on a single system than on many systems that are located on the same network site. An UTM system usually has a firewall, functionality for malware detection and deletion, for detecting and blocking dangerous programs, and so on. There are several advantages and disadvantages for merging functions into a single system. For example, the implementation of an UTM reduces complexity by making a single system responsible for many objectives, but also requires that UTM has all the qualities needed to achieve each of the objectives. Another aspect relates to performance: a single system that manages some work needs to have enough resources like CPU speed and memory for any work.

2.1.9 Web application firewalls

HTTP protocols used on the web server have been exploited by attackers in many ways, such as setting up a malicious program on someone's computer by surfing the web or deceiving a person for discovering private information they have not changed . Many of these uses can be detected by specialized firewall applications called web application firewalls that stay ahead of the web server.

Web application firewalls are relatively new technologies compared to other firewall technologies and the types of threats they can reduce are still changing frequently. Because they are placed at the web server's input to prevent attacks on it, they are considered different from traditional firewalls.

2.1.10 Firewalls for Virtual Infrastructures

Many virtualization solutions allow more than one operating system to be executed simultaneously on a single computer, where each one behaves as if it were a real computer. Recently, this has started to be used frequently because it enables efficient use of hardware resources. Many of these types of virtualization include network virtualization, which allows multiple operating systems to communicate as if they are on an ordinary Ethernet network, although there is no network device.

Network activity that goes directly to the virtualized operating system of the host can not be monitored by an external firewall. However, many virtualization systems often have prior configured firewalls or allow third-party software to be plugged in. Using firewalls for

monitoring virtual networks is relatively a new field of firewall technologies, and this is likely to change considerably watching increased use of virtualization.

2.2 Firewall Inspection Restrictions

Firewalls can only work efficiently in that traffic they can monitor. Despite the choice of firewall technology, a firewall that does not understand the traffic flowing through it will not handle traffic properly. For example, allow traffic that should have been blocked. Many network protocols use cryptography to hide traffic data. Firewalls can also not read encrypted data such as emails that are encrypted using S / MIME or OpenPGP protocols or files that have been manually encrypted. For example. IPv6 can be "tunneled" in IPv4 in many different ways.Content may still be not encrypted but if the firewall does not understand the part used for tunneling, traffic can not be interpreted.
In all these cases, firewall rules will determine what should be done with encrypted traffic or with traffic that is not encrypted. All institutions should have policies about handling traffic in such cases as permitting or blocking encrypted traffic that is not authorized to be in that way.

2.3 Summary of the Rules

The following items summarize the key recommendations from this chapter that are compulsory for implementation:
- Using NAT should be considered a routing form, not a firewall type.
- Institutions should only allow only the incoming traffic that uses source IP addresses that are in use by the institution.
- Compliance check is useful in a firewall only when it can block communications that can be harmful to system defenses.
- When choosing the type of firewall to use, it is important to decide whether it should behave as a proxy for applications.

3. Firewalls and Network Architecture

Firewalls are used to separate nets with different security requirements, such as the Internet and the internal network that holds the server with sensitive data. Institutions should use firewalls where the network and the internal system encounter network and external systems, and where security requirements change from internal network. The purpose of this section is to help institutions determine where a firewall should be placed and where to place other systems and networks that are connected with the firewall.
Since one of the main functions of a firewall is to prevent access to unneeded traffic to the network firewall, the firewall should be located at the boundaries of the logical network. This normally means that firewalls are positioned either as a node where the network is shared across multiple paths, or in the single path line. In routed networks, the firewall generally stays in the place just before the traffic enters the router and is sometimes associated with the router. It is very rare to set up the firewall in multi-path mode after the router because the firewall device will need to see every path that exists in a typical situation. Most hardware firewalls have

routing capability, and in a network switch a firewall is often part of the switch itself to provide protection as much as possible.
Firewall manufacturers often vary in their terminology in the logical flow of firewall traffic. A firewall receives traffic that has not been checked, checks it according to firewall policies and then traffic passes according with circumstances(for example, allows traffic to pass, block it, passes it after making some modifications). Because all network traffic is in one direction, the policies are based on the traffic direction. For purposes of this regulation, traffic that is not controlled yet comes from the "unprotected" side of the firewall and is moving toward protected side. Some firewalls control traffic in both directions.
Chapter 2 lists many different types of firewall technologies. Network firewalls are almost always hardware devices with multiple network interfaces, host-based.

3.1 Network Models with Firewalls

Figure 3.1 provides a typical network model with firewall hardware device that acts as a router. The unprotected firewall side is connected to a single path called 'WAN' and the protected side is connected to three paths called 'LAN1' (local area network), 'LAN2' and 'LAN3'. The firewall acts as a router for traffic between wide-area wide area network (WAN) and LAN paths. In this figure one of the LAN paths also has a router, some institutions prefer to use multiple layers of routers due to inherited routing policies inside the network.

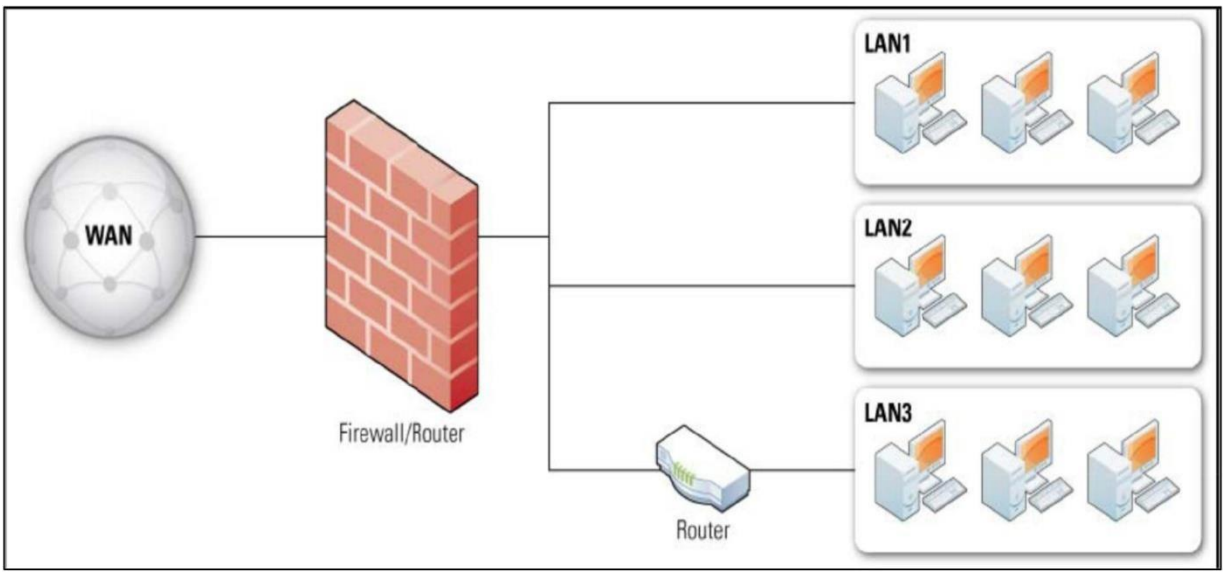


Figure 3.1 A network routed with firewall devices

Many firewall devices have a feature called DMZ, acronym that is connected to demilitarized areas. While there is no single technical definition for firewall DMZs, they are generally routing interfaces similar to the interfaces found on the firewall's protected side. The main difference is that the traffic that moves between the DMZ and other interfaces on the firewall's protected side goes through the firewall and may have firewall protection policies applied. DMZs are sometimes needed for those institutions whose traffic should bypass some of the firewall policies (for example, because the DMZs are highly hardened), but the traffic coming from

other systems should definitely pass through the firewall. Setting up servers, such as web and mail servers, in the DMZ is common. An example of this is shown in Figure 3.2, a simple network model with a DMZ firewall. Internet traffic goes through the firewall and is routed to the firewall protected system or to the DMZ system. The traffic between the DMZ system and the protected network system runs through the firewall and may have firewall policies applied.

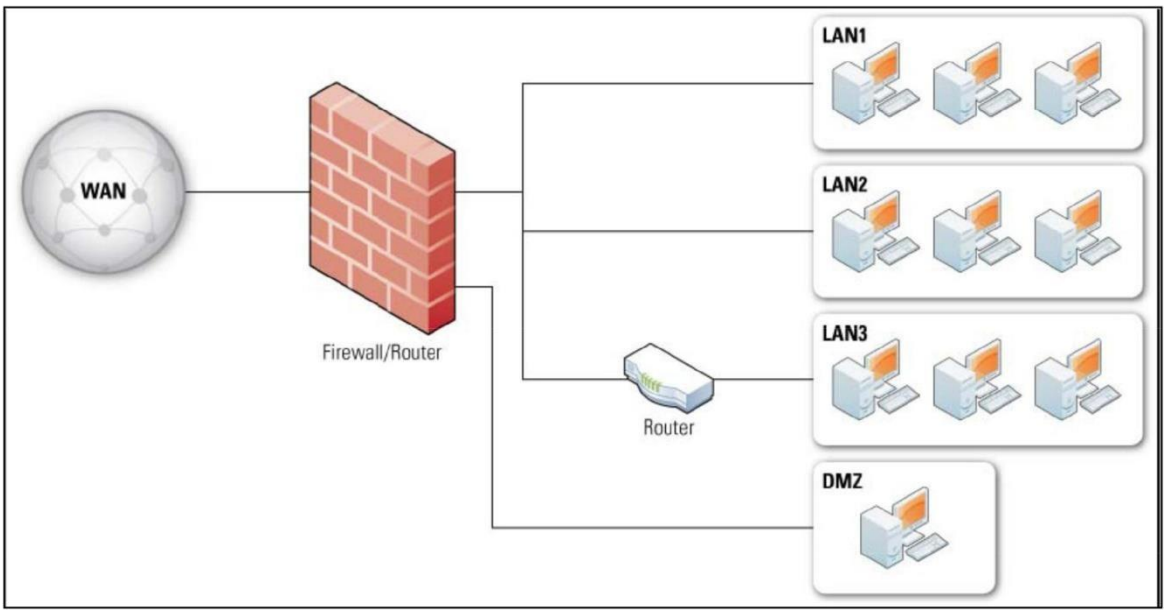


Figure 3.2 Firewall with DMZ

Many network architectures are hierarchical, meaning that a single path from an external network is devided on many paths in the internal network and it is generally more efficient to set up a firewall in the path where the path is devided. However, there may be reasons to have an additional firewall inside the network, such as to protect one computer community from another. If the network architecture is non-hierarchical, the same firewall policies can be used on all network entries. In many institutions it is supposed to be just a network entry, but other entries have been raised to a basic ad hoc, often in ways that are not allowed by general policies. In this situation, if a properly configured firewall is not located at any entry point, malicious traffic that will normally be blocked by the main entrance can enter the network in other ways. The diagrams in Figures 3.1 and 3.2 show each one a simple firewall; however, many implementations use multiple firewalls. Some manufacturers sell high-availability firewalls, which allow a firewall to take over another even if the first firewall fails or is kept offline for maintenance purposes. High availability firewalls are placed in pairs at the same location on network topology so that they both share the same external and internal connections. While high availability firewalls can increase reliability, they can also bring some problems, such as the need to combine logs between paired firewalls and possible administrator confusions when configuring firewalls. Firewall functionalities with high availability can be provided by various techniques of specific manufacturers.

3.2 Firewalls that act as Network Address Translators

Many firewalls can perform NAT (Network Address Translator) . NAT is not part of the firewall's security functionality. NAT's security benefit is that the prevention of contact between a host outside of a firewall with a host behind NAT can be achieved easily from a firewall without the help of protocols that do not work well behind NAT. However, NAT activation on a firewall is simpler that proper configuration of firewall policies to have the same protection, so most people think that NAT is the main security feature.
Generally, a NAT acts as a router that has a network with private addresses and a single public address on the outside. The way a NAT does these address translations many to one varies from implementation, but almost always includes the following elements:

- Hosts inside the network initiate a connection with external network by causing NAT to determine the source ports for connection different from those controlled by NAT. NAT uses the source port number to determine connections from outside to inbound hosts.
- Hosts outside the network can not initialize contacts with hosts inside the network. In some firewalls, NAT may be configured to define a special NAT destination port to a specific host inside NAT, for example all HTTP requests that go to NAT can be addressed to a unique host on the protected side of the firewall. This quality is often called pinholing.

Although NATs are not features of a firewall, they interact with firewall security policies. For example, there are policies that require all accessible HTTP servers to be in DMZ, and should prevent NAT from pinholing TCP at gate 80. Another example that NAT interacts with security policy is the ability to identify the traffic source in a firewall's logs. If a NAT is in use, it should report private addresses to the log instead of the translated public addresses, otherwise the logs will mistakenly identify many hosts from a single public address.

3.3 Multilayer firewalls architecture

There is no restriction on where the firewall will be placed on a network. While firewalls should be in the boundaries of a logical network, creating an "internal" and "external" boundary on both sides of a firewall, a network administrator may want to have additional boundaries within the network and put additional firewalls on such boundaries. Using multiple layers of firewalls is quite common to provide more protection.
A typical situation that requires multiple layers of firewall networks is the presence of internal users with different levels of trust. For example, an institution may want to protect the accounting database from being accessible to users who are not part of the Accounting Department. This can be realized by placing a firewall at the network boundary (to prevent general network access from the Internet) and another at the boundary of the internal network that limits the Accounting Department boundary. The internal firewall can block access to the database server from outside the network, while allowing limited access to other resources on the network. A typical use for firewalls inside the network with side firewalls includes visitors who need Internet access.
Placing a firewall inside a network that has another firewall on its boundary requires good planning and policy coordination to prevent unintentional mistakes in security. A better treatment is duplication of external firewall policies, which are also important for internal

firewalls. This may be difficult if the firewalls are unable to coordinate their policies automatically, which is possible when firewalls belong to different manufacturers.
Another common problem with the use multi layers firewalls is the increased difficulty that comes in finding firewall problems. If a firewall stays between a user and a server, and the user can not connect to the server, it's easy to check the firewall logs to see if the connection is allowed. But if too many firewalls are involved, the problem is getting harder because an administrator needs to locate the whole chain of firewalls and check their logs to find out the origin of the problem. The presence of multi application-proxy gateway layers is particularly worrying because any gateway can change a message, which makes it even harder to trace.

3.4 Summary of the Rules

The following items summarize the main recommendations from this chapter:

- The firewall needs to fit with the current network model. However, an institution may change its network architecture at the same time that it places a firewall as part of overall security improvement.
- Certain common network architectures lead to different solutions for placing firewalls, so an institution should evaluate which architecture works best for its security purposes.
- If a side firewall has a DMZ, it should be determined which of the services should be implemented by the DMZ and which should stay inside the network.
- Do not rely on NAT to provide firewall benefits.
- In some environments, placing firewalls one after the other can boost the desired security, but in general such multiple layers of firewall can increase complexity.

4. Firewall Policies

A firewall policy shows how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on institution information policies. Before the firewall policy is created, a risk analysis should be done to create a list of necessary traffic for the institution and categorize them how to be safe- including those types of traffic that pass through the firewall and what circumstances go by. This risk analysis should be based on the evaluation of threats and vulnerabilities: countermeasures in order to reduce the vulnerabilities; and the impact when the system or data are compromised. Firewall policies can be documented in the system security plan, maintained and up-to-date as attacks and vulnerabilities increase. The policy should include specific guidelines on how to address changes in the set of rules
Generally, firewalls can block all incoming and outgoing traffic that is not allowed by firewall policy - traffic -that is not needed for the institution. This practice is known as the default block, reduces the risk of attacks, also reduces traffic to the institution's networks. Due to the dynamic nature of hosts, networks, protocols, and applications, default blocking is safer than allowing all traffic that is not explicitly prohibited.
This chapter provides details on what types of traffic should be blocked.

4.1 Policies based on IP addresses and protocols

Firewall policies should only allow protocols of necessary IPs. Common examples of IP protocols used are: ICMP, TCP, and UDP. Other IP protocols such as IPsec, ESP (Encapsulating Security Payload), and AH (Authentication Header) and routing protocols have to pass through the firewall. These necessary protocols should be limited whenever possible in specific hosts and networks inside the institution with the need for their use. By allowing only the necessary protocols, all unnecessary IP protocols are automatically blocked.

4.1.1 IP Addresses and Other IP characteristics

Firewall policies should only allow the use of appropriate IP source and destination addresses. Specific recommendations for IP addresses include:

- Traffic with invalid sources or destination addresses should always be blocked, regardless of the location of the firewall.
- Traffic with an invalid source address for incoming traffic or invalid destination address for outbound traffic should be blocked on the perimeter of the network. This traffic is often caused by malicious software, spoofing, DoS attacks, or unconfigured devices.
- Traffic with a private destination address for incoming traffic or source address for outgoing traffic should be blocked on the network's perimeter. Network perimeter devices can perform address translation services to allow private hosts to communicate through the perimeter, but private addresses should not pass through the network perimeter.
- Outbound traffic with invalid source addresses should be blocked. This is often called outbound filtering. Systems that are compromised by attackers can be used to attack other systems on the Internet; using invalid source addresses makes much more difficult to stop these attacs. Blocking this type of traffic on an institutional firewall helps to reduce the effectiveness of these attacks.
- Incoming traffic with firewall address destination should be blocked, only if the firewall offers incoming traffic services that require direct connection - for example if the firewall is acting as an application proxy.
- Traffic containing routing information for IP sources, which allows the system to specify the router that the packets will use as they go from source to destination. This can potentially allow an attacker to build a package that skips network security controls. Routing the IP sources are rarely used in modern networks.
- External network traffic contains broadcast addresses that are directed to the inside network. Any system that responds to the broadcast will send its response to the source-specified by system instead of the source system. These packages may have been used to cause large network traffic storms through DoS attacks. The normal address transmission, as well as the addresses used for IP multicast, may or may not be suitable for blocking the institution's firewall.

Firewall in the network perimeter should block all incoming traffic to networks and hosts that need to be inaccessible from the external network. These firewalls should also block all outbound traffic from the institution network and hosts that should not be allowed to access the external network. Deciding which of the addresses should be blocked is often one of the aspects

that take more time to develop firewall IP policies. This aspect is also one of worst because the IP address associated with an unwanted entity often changes over time.

4.1.2 IPv6

IPv6 is the new version that is being implemented more and more. Although the IPv6 internal length format changes from IPv4, many other features remain similar. For similar qualities among them, firewalls should work alike. For example, blocking all incoming or outgoing traffic that is not allowed by firewall policy will be accomplished regardless of the IPv4 or IPv6 address version.
Thus, some firewalls do not handle IPv6 traffic at all; others treat but have traffic filtering limitations; and others can filter it similarly to IPv4 traffic. All institutions that decide whether or not to allow IPv6 traffic on the internal network should implement a firewall that is able to filter traffic. These firewalls should have the following capabilities:

- The firewall should be able to use IPv6 addresses in all filtering rules that use IPv4 addresses.
- The administration interface should allow the administrator to clone IPv4 rules for IPv6.

4.1.3 TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)

Application protocols can use Transmission Control Protocol (TCP), UDP (User Datagram Protocol) or both, depending on the protocol construct. An application server usually hears one or several fixed TCP or UDP ports. Some applications use a single port, but most applications use many ports. For example, although SMTP uses the TCP 25 port to send email, it uses the TCP 587 port to receive e-mail. FTP (FileTransfer Protocol) uses at least two ports, one of which can be unpredictable, and while most web servers use only TCP 80 port, it is common to have web pages that use other ports such as TCP 8080 port. Some applications use TCP and UDP together; for example DNS lookup can occur at UDP 53 port or TCP 53 port.
As with other aspects of firewall rules, deny by default should be used for TCP and UDP inbound traffic. Less strict policies are commonly used for TCP and UDP outbound traffic, because most institutions allow their users to access a wide range of applications localized on millions of external hosts.
Except allowing and blocking UDP and TCP traffic, many firewalls are also capable of reporting or blocking malicious UDP and TCP traffic directed at firewalls or at hosts that are protected by firewalls. This traffic is often used to scan hosts, and is likely to be used by certain types of attacks. Firewall can help block such activities - or report when activities take place.

4.1.4 ICMP (Internet Control Message Protocol) Basic Internet Protocol used for the exchange of error messages

Attackers can use different types of Internet Control Message Protocol (ICMP) and codes to detect or manipulate the traffic flow. However ICMP is needed for many useful things, to get a reasonable performance on the Internet. Some firewall policies block all ICMP traffic, but this often displays problems with diagnostics and performance. Other common policies allow all ICMP outbound traffic, but limit the incoming traffic for these types.

To prevent malicious activities, firewalls in the network perimeter should deny all ICMP incoming and outgoing traffic except those types and codes that are specifically allowed by the institution. For ICMP in IPv4, 3 ICMP messages should not be filtered because they are used for important network diagnostics. Ping Command (ICMP 8 Code) is an important network diagnostic, but incoming pings are often blocked by institution policies to prevent attackers learn more about topology of the network of the institution. For ICMPs in IPv6 should be allowed many types of messages in specific circumstances to enable different IPv6 features.
ICMP is often used by low-level network protocols to increase network speed and reliability. Therefore, ICMP on an institution's network generally should not be blocked by firewalls that are not in the network's perimeter, except when security needs weigh more than the network's operational needs. Similarly, if an organization has more than one network, ICMP coming or going to other networks within the institution should not be blocked.

4.1.5 IPsec protocols

An institution needs to have a policy to allow or not IPsec VPNs that start or end inside the network's perimeter. ESP and AH protocols are used for IPsec VPNs, and firewalls that block these protocols will not allow IPsec VPN to pass. While ESP is blocked, it may prevent encryption to protect sensitive data, and may also force users who will normally encrypt their data with ESP to allow it to be inspected.
Institutions that allow IPsec VPNs should block ESP and AH except those who direct and come from internal network addresses - these addresses belong to the IPsec ports that are allowed to be the VPN endpoints. By applying these policies, employees will be required to familiarize themselves with the policy to open ESP and / or access AH to IPsec routers inside an institution. This will also reduce the amount of encrypted traffic from within the network and that can not be considered by network security controls.

4.2 Application-Based Policies

At first, firewalls were used simply to block unwanted or suspicious traffic on the network boundary. Nowadays they have another use, they allow traffic destined for a particular server within the network, but they catch that traffic on a server that processes it like a port-based firewall. The theory is that application or proxy firewalls can protect the server better than the server protects itself - and can also remove the malicious traffic before it reaches the server, helping to reduce server load. In some cases, an application or proxy firewall can remove that traffic that a server can not delete itself because it has very good filtering capacity. An application or proxy firewall can prevent the server from direct acces of the external network. If possible, incoming firewall and proxy applications should be used for any server that does not have sufficient security to protect against typical attacking applications. The main conditions to decide when to place a firewall or proxy application or not are:

- Is a suitable application firewall available? Or if appropriate, is there a suitable application proxy available?
- Is the server protected enough by existing firewalls?

- Is it easy to update filtering rules on the main server and in the firewall or proxy application to handle the recent threats?

Application proxies may cause problems if they are not suitable. Only if it is updated and more efficient than the server can continue to be used. Application firewalls can also cause problems if they are not fast enough to handle server-targeted traffic. However, it is important to consider server resources, if the server has enough resources to handle potential attacks, there is no need to use the application firewall or proxy.
When an application firewall or proxy entry is behind the firewall or firewall perimeter DMZ (demilitarized zone), the perimeter of the firewall should implement blocking based on the IP addresses, described earlier in this section to reduce the load on the application's firewall or proxy. Outbound traffic proxy applications are useful for detecting those systems they are doing inadequate or dangerous connections from the inside of the protected network. So far the most usual outbound traffic proxy is HTTP. They allow an institution to filter dangerous content before they reach the required PC. Also they help one institution to better understand web traffic from its users, and to detect activities that have begun to pass through HTTP. When an HTTP proxy filters the content it can notify the user that the site that was visited has sent filtered content.

4.3 User Based Identity Policies

Traditional packet filtering can not look at the identity of the users that are communicating in traffic by passing the firewall, so firewall technologies can not have policies that allow or refuse access based on these identities. However, many other firewall technologies can see the user's identity, so they approve policies based on their authentication. One of the most common ways to implement the user identification policy is through the use of VPN. Like IPsec VPNs as well even SSL VPNs have different ways of authenticating users, such as with multi-factor authentication or the use of digital certificates that are controlled by each users. NAC is also a common method for firewalls that allows or denies access of users to certain network resources. Firewalls that apply user - driven policies should reflect them in their logs. This means that it is not enough simply to have a log out of the IP address from which one certain user is allowed to have access to the policies, but it is also important that to know the identity of the user.

4.4 Policies based on network activity

Some firewalls allow the administrator to block established connections after a certain period of time passivity. For example, if a user outside the firewall is logged on the server files, but did not make any requests over 15 minutes, policies can block any further communication of that link. Time - based policies are useful in preventing attacks caused by login of users who are away from the computer for a certain time and another user who is sitting and is using the connection. However, these policies may also not be appropriate for the user who make connections, but do not use them often. For example, a user can connect with a file server to read a file and then spend a lot of time to edit file. If the user does not save the file to the server before the firewall expires of active attitude, the changes made will not be saved.

4.5 Summary of the Rules

The following items summarize the main rules of this chapter, mandatory for implementation:
- The firewall policy of an institution should be based on an overarching analysis risk.
- Firewall policies should be based on blocking all incoming or outgoing traffic, making the exception for the desired traffic.
- Policies, apart from content, should consider source and destination traffic.
- Many types of IPv4 traffic, such as invalid or private addresses, should be blocked in the basic configurations.
- Institutions should have policies for handling IPv6 incoming and outgoing traffic.
- An institution needs to determine which application can send traffic inside or outside its network and make firewall policy for blocking other applications.

5. Planning and Implementing Firewalls

This chapter focuses on planning and implementing firewalls. With the application of a new technology, planning and implementation of firewalls should be handled in phases. If a clear planning is followed step by step, successful implementation can be achieved. Phased implementation can minimize unforeseen issues and identify earlier potential threats. This chapter examines in depth any planning of firewalls and phases of the implementation, including:

1. **The plan.** The first stage of the process is to identify all the requirements that one institution should consider when determining which of the firewalls should be implemented to enforce the security policies of an institution.

2. **Configuration.** The second stage has to do with all aspects of the platform's configuration firewalls. This includes installing hardware and software as well as setting up system rules.

3. **Testing**. The next stage is to implement and test the designed solution. The main goals of the test are to evaluate functionalities, scalability and security of solution and to identify such issues like interaction with components.

4. **Setting.** Once the testing is completed and all issues are resolved, the next phase focuses on setting up firewalls.

5. **Management.** Once the firewall is set up, it is managed throughout the life cycle, including component maintenance and support for operational issues. This lifecycle process is repeated when important improvements or changes are needed to be included in the solution.

5.1 The plan

The planning phase for firewall selection and implementation should only start after an institution has determined what is required for a firewall to implement security policies. This usually occurs during a risk assessment for the entire system. A risk assessment includes:

1. Identification of threats and weaknesses in the information system;
2. Possible impacts or extent of damage from loss of confidentiality, integrity and availability of the institution's assets or operations;
3. Identification and analysis of security controls for the information system;

The basic principles that institutions have to follow in planning firewall deployment include:

- **Use of equipment as they are intended to be used.** Firewalls should be used only as firewalls. Additionally, firewalls should not be expected to offer non-security services such as: act as a web server or e-mail server.
- **Creating in-depth protection.** In-depth protection involves the creation of many layers of security. This allows the risk to be more manageable, because if a layer of protection is compromised, another layer is there to stop the attack. In the case of firewalls, in-depth protection can be accomplished by using multiple firewalls along the institution, including the perimeter, in front of the sensible departments in the interior, and in any individual computer. For in-depth protection to be more effective, firewalls should be part of a general security program that includes products such as, programs which enable control, identification, elimination of computer software maliciously installed on computers (virus, trojan, etc) and intrusion detection programs.
- **Pay attention to internal threats.** Focusing your attention only in external threats can be left a wide open net for attacks from inside. These threats can not come from within, but may include the host intrinsically infected by malware or malware compromised by external attacks. Important internal systems should be placed behind the internal firewalls.
- **Document the capabilities of firewalls**. Each model of firewalls has different capabilities and limitations. These affect the planning of the institution 's security policies and on firewall distribution strategy. Any characteristic that affects positively or negatively in planning should be written in the overall planning document.

Remember that the phrase "All rules are made to be broken" applies when firewalls are implemented. While firewall implementers should keep in mind the above rules during planning, each network and institution has special requirements that may require special solutions.

Institutions when they want to make the purchase and implementation of firewall solutions should take consider the following points.

- Security Capacities

- Which area of the institution should be protected (perimeter, internal departments, specific services etc.)?

- Which types of firewalls technologies will better address the types of traffic to be protected (packet filtering, inspection, firewall applications, proxy-gateway applications, etc.)?

- What additional security features - such as intrusion detection capabilities, private network virtual (VPN), and content filtering - does the firewall need to support?

▪ Management

- Which protocols support remote management firewalls, such as HTTP over SSL, SSH, or access to serial cable?
- Are remote management protocols acceptable for use based on policies of the institution?

- Can remote access be limited to some firewall interface and IP source address like those in the internal network?

- Is central firewall management allowed by the same manufacturer?

- If this management is possible should any particular application be required by the manufacturer or other apps can be used?

▪ Performance

- What amount of transmission, number of simultaneously connections, connections per second and delays are allowed so that the firewall does not turn into a network access blocker, for current traffic and what is expected in the future?

- Are the number of failures and loads required as a factor to ensure high availability?

- Should you consider whether the firewall is hardware-based or software-based?

▪ Integration

- Will firewall need special hardware to integrate into one's network institution?

- Should the firewall be compatible with other network devices that provide security either other services?

- Does the logon of firewalls communicate with other logging systems?

- Do we need to change the network space to install the firewall?

▪ Physical environment

- Where to place the firewall physically in order to have physical security and protection against natural phenomena?

- Is there enough space where it will be placed?

- Will there be additions to electrical power, backup, conditioning and physical connections in the physical environment where the firewall will be installed?

▪ Staff

- Who will be responsible for firewall management?

- Do the system administrators need training before the firewall is installed?

▪ Future requirements

Does the firewall meet the requirements of the institution in the future, such as the implementation of IPv6 or the growth of bandwidth? The following requirements should be considered when purchasing and installing firewalls host-based or personal:

- Do servers and computers where it will be installed fulfill the minimum firewall requirements?

- Will it be compatible with other security software on the server or workstation?

- Can the firewall report policy breaks to a central server?

- Can it be locked so that only administrators can modify it?

- Will the firewall conflict with other firewalls installed on the operating systems of hosts?

5.2 Configuration

The configuration phase includes all the steps of configuring the firewall platform. It includes installation of hardware and software, policy configuration, log configuration and alarms and firewall integration in network architecture.

5.2.1 Hardware and software installation

Once the firewall is purchased and selected, the operating system must be installed on a software-based firewall. Then install the patch and make updates. Among this time the firewall needs to be strengthened to reduce the risks to it and the operating system. Remote access consoles should also be installed.

During installation and configuration, only administrators should have access to the firewall. All the management parts, such as SNMP, should be disabled if not needed. If the firewall allows special account administrator, then it must be configured one by one.

Network firewalls should be placed in rooms that meet the vendor's related recommendations with temperature, humidity, space, energy, etc. The room also needs to be necessary safety to prevent unauthorized personnel from accessing the firewall.

Comparing logs from different sources is very important when analyzing, therefore the internal clock of each firewall should be consistent with other systems institution. This is achieved through a central authority that makes synchronization.

5.2.2 Policy Configuration

After installing and securing the hardware and software the administrators have to create policies. Some firewalls implement policies with specific rules, some require firewall configuration and create rules themselves, some creates them automatically, some others combine all three techniques. Conclusion is a set of rules that describe how the firewall will behave.

These "rule sets" should describe the institution policies and policies specified in security plan. To create this set of communiques, the types of traffic should be defined for applications approved by the institution. This should include the protocols the firewall needs for daily work.

The details of creating rules depend on the type and the specific product. For example a lot firewalls control traffic through rules sequentially. For these firewall the rules with the highest probability should be placed as above in the list.

They also are useful to employees who audit the rules. Although the comments look like important they have plenty of value over time. Also the change of the rules and comments should be kept in certain logs.

At least the following rules should be noted:

- Port filtering must be enabled for the outside of the network and in some parts inside it.
- Content filtering should be as frequent as possible.

There are many ways to set rules and every institution should have the requirements and persons involved in this process.

If some rules are the same for some firewalls then they need to be synchronized. This is done according to what the seller has allowed. It should be noted that some firewalls have policies depending on the location of the institution network.

5.2.3 Configuring logs and alarms

The next step is configuring logs and alerts. The log is a critical step for fixing in case of failures and is needed to make sure that the security configuration is correct. If it is done properly, the log helps greatly to investigate and resolve incidents. When is it the possible firewall should store them locally and send them to a central infrastructure.

If the firewall allows accounts with different rights, it must create one that has only one right reading, for log analysis. This account can also be used for auditing and when only reading rights are needed. In addition to logs, alarms must be configured. They may include:

- Any modification or deactivation of firewall rules
- Restart, lack of memory or other operational problems
- Other status changes, if allowed.

5.3 Testing

The new firewall must be tested and evaluated before installation in order to ensure that works correctly. Testing should be carried out in a testing environment free from production environment. This test should attempt to replicate the production environment as near as it is possible. The aspects of the solution to be assessed are as follows:

- **Connections.** Users can set up and maintain connection through the firewall.

- **Community of rules.** Only traffic that is compatible with the security policy is allowed. The one who is not allowed is banned from the firewall. Verification of the rules includes manual verification and testing if they work properly.

- **Compatibility with applications.** Personal or host-based firewalls do not interfere with existing apps. This also includes network communication between application components.

- **Management.** Administrators can manage and configure the solution in a safely way.

- **Login.** Logging and management functions are consistent with policies and strategies of the institution.

- **Performance.** The solution offers acceptable performance under normal conditions and heavy traffic. In such cases it is good to use traffic generators for the size of the normal cases or heavy traffic. The Simulated Distributed Denial-of-Service (DDoS) can also help in evaluating performance. Testing should include types different applications that pass through the firewall, especially those that create delays.

- **Security of implementation.** The firewall itself can have weaknesses that can be used by attackers. High security institutions should test firewalls themselves and his parts.

- **Connecting components.** Different parts of the firewall solution need to communicate without problems, this is very important when parts are from different manufacturers.

- **Policy Synchronization.** If there are some firewalls that have synchronized policies they need to test these policies in different scenarios.

- **Additional functionalities.** Additional functions, such as virtual private network (VPN) or programs that enable the control, identification, elimination of harmful computer programs installed on computers (virus, Trojan etc), should also be tested.

5.4 Installation

After testing has been completed and all issues are resolved, the next planning phase and firewall implementation is the placement that needs to be done in accordance with the company policies. Before setting up the firewall, administrators should alert the user or system owners who have the potential to be affected by changes, over the planned deployment, and guide who should be notified if they pose a problem. Also other changes needed for other devices should be coordinated as part of the firewall deployments. The security policies that are expressed through the configuration of the firewall should be added other company security policies, and

the ongoing changes to configurations should be integrated with the organization's configuration management processes. If multiple firewalls are installed, including personal or branch firewalls in different offices, a gradual or phased approach should be considered; Also, a pilot program could be useful, especially to identify and resolve policy issues that are facing each other. This will provide administrators an opportunity to assess the impact of firewall resolution and will resolve potential issues before placing the entire company.

Connecting a firewall to an institution network requires more than just deciding firewall in the flow of external traffic, network integration is also included firewall with other network elements that will interact with the firewall. Given that firewalls are typically behaved as routers, the firewall should be integrated into the route structure of the network. This usually means replacing any router that is in the same position on network topology such as firewall deployment, but may also need to change the route charts so that the other network routers of the institution to withstand the addition of this new router. If network elements use their dynamic route, these elements may need to be altered in order to be aware of them firewall route. Also, the network switch from the outside of the protected network may need to be reconfigured to handle firewall addressing. If the firewall is a system set with prediction of system failures, the network switch can should be configured to cope with possible failures.

5.5 Administration

The last phase is also the longest phase and is that of post-settlement management implementation. It includes the maintenance of architecture, rules, policies, software and all other parts of the solution. One case is when different patches should be selected and implemented. Another case is updating various rules. Performance of the firewall should be constantly monitored just like logs and alarms. Also rules and configuration should be backed up on a continuous basis. It is best to look at firewall policies in a regular manner. Each review should have one list with all the changes observed since the last audit. Possibly external experts should make audits in rare cases. Some tools allow automatic audits for unnecessary rules or for recommended but missing rules. If such tools are available, they should be used regularly. Institutions need to take in consideration carrying out various tests for penetration in order to assess the safety of their overall network. These tests let you know if the rules set of the firewall are operating properly. They should be used in addition to ordinary audits and not to replace them.