The policy discussed suggests that the network be partitioned into several parts with guards between the various parts to prevent information from leaking from one part to another. One part of the network will be available to the public, and a second part will be available only to the company employees. This is a fairly standard corporate network architecture. This architecture is depicted in the graphic below.

**Def:** The *DMZ* is a portion of a network that separates a purely internal network from an external network.

The DMZ separates the company’s network from the internet. Any customer interaction with the company will occur in the DMZ. Thus, web servers that supply public information to the customer about company products and web servers that accept customer orders are located in the DMZ. We will describe later the specific functions of the Outer and Inner Firewalls.
Firewalls and Proxies

The guards that support the access control mechanisms to implement the developed security policies are the firewalls, both outer and inner, and the proxy services.

**Def:** A *firewall* is a host that mediates access to a network, allowing and disallowing certain types of access on the basis of a configuration security policy.

It accepts or rejects messages based on external information, e.g. destination addresses or ports, rather than on content of the messages. It also accepts or rejects messages based on the origination address or port.

**Def:** A *filtering firewall* performs access control on the basis of attributes of the packet headers such as destination addresses, source addresses, and options.

Routers and other infrastructure systems are typical examples of filtering firewalls. They allows connections through the firewall based on source and destination addresses and ports.

**e.g.**

TECNET router

**Def:** A *proxy* is an intermediate agent or server that acts on behalf of an endpoint without allowing a direct connection between the two endpoints.

**e.g.**

TECNET Proxy
Def: A proxy (or applications level) firewall uses proxies to perform access control. A proxy firewall can base access control on the contents of packets and messages as well as on attributes of the packet headers.

A proxy firewall adds to the filtering firewall the ability to base access on content either at the packet level or at a higher level of abstraction.

Analysis of the Network Infrastructure

The security policy benefits from the design flow of information and the principle of least privilege. The policy distinguishes public entities from those internal to the corporation. It recognizes that some company resources must be available to the public. The public entities may enter the company’s perimeter but are confined to the DMZ.

The key decision is to limit the flow of information from the internal network to the DMZ. The public cannot communicate directly with any system on the internal network, nor can any system on the internal network communicate directly with any system on the Internet. The systems in the DMZ serve as mediators with the firewalls providing the guard function. The firewalls and the DMZ control all access to and from the Internet and filter all traffic in both directions.

The first step is to conceal the addresses of the internal network. A typical approach is to assign each host on the internal network an address but to not allow those addresses to leave the internal network. This is accomplished by the inner firewall.

The DMZ mail server is the corporate mail server when viewed from the public. All mail into the company goes to this mail server. The DMZ mail server then forwards the public mail to the correct company recipient. Conversely, when someone in the company sends an e-mail to the Internet from the corporate network, that e-mail is routed through the DMZ mail server. For outgoing e-mail all e-mail would be routed to the DMZ mail server. That server would need to change any internal address to the external address for the DMZ mail server before sending the e-mail to its recipient.

The Web server resides in the DMZ to prevent unwanted access to the internal corporate network.

Outer Firewall Configuration

The goals of the outer firewall are to restrict public access to the corporate network and to restrict employee access to the Internet. Thus, it is blocking information in both directions. There has been a corporate decision that no company employee will access the Internet from the company’s internal network. The outer firewall implements this policy. Additionally, only e-mail and well-formed web addresses to the web server are allowed through the outer firewall from the Internet to the DMZ.

The firewall is also a proxy-based firewall in that when an e-mail connection is made, the SMTP proxy on the firewall collects the mail. It analyzes that e-mail for computer viruses and other forms of malicious logic. If none is found, that e-mail is forwarded to the DMZ mail server. The outer firewall also scans incoming web connections for any suspicious components. If none is found, the outer firewall forwards the connection to the DMZ web server.

Attackers may try to penetrate the firewall using any one of three methods.

1. Enter through the Web Server port (HTTP & HTTPS)
   The firewall checks for legal, well-formed HTTP(S) requests. Only legal, well-formed HTTP requests are forwarded to the DMZ Web server.
2. Enter through the SMTP port
   The mail proxy will detect such an attempt and reject such attempts.

3. Bypass the low-level firewall checks and exploit vulnerabilities in the firewall
   The system admin will update the firewall software frequently.

**Inner Firewall Configuration**

The company’s internal network is where the most sensitive data is stored. Hence, the inner firewall must block all network traffic that tries to access the internal company network. Additionally, the inner firewall restrict the network traffic that is initiated from the internal network to e-mail to the DMZ mail server, limited ssh traffic to the Web server in the DMZ and limited ssh administrative access to the computers in the DMZ. All other traffic from the internal network to the DMZ or beyond is blocked.

**Goal**

Block all traffic except that specifically authorized and then only from DMZ, never from the internet

- **Good?**
- **Bad?**
  - remote support

**The DMZ**

Four systems reside in the DMZ: mail, WWW, DNS, and log servers.

**DMZ Mail Server**

- Performs address and content checking
- Hide information from outside world
- Be transparent to the inside

Mail from the Internet to the company

1. Reassemble the message into a set of headers, a letter, and any attachments. This simplifies checking.

2. Scans e-mail and attachments looking for bad stuff
   - virus
   - malicious logic
   - no binary data

3. Scans recipient address lines and redirects mail to internal server

Outgoing mail from one of the company’s internal e-mail servers to the Internet

1. Reassemble the message into a set of headers, a letter, and any attachments. This simplifies checking.

2. Scans e-mail and attachments looking for bad stuff
   - virus
malicious logic
no binary data

3. Scans all header lines and changes all internal hosts to company.org

Goal
Handle all Mail
Perform all checks and sanitizations

Also run SSH on mail server to only accept connections from trusted administrative host(s) on the internal network.

DMZ WWW Server

The DMZ web server contains only public information that the company wants to distribute. Additionally, no confidential data is ever present on the DMZ Web server. The DMZ Web server also acts as the interface with the company’s customers in their ordering products from the company. Thus, private customer data may temporarily reside on this server. The server uses the IP address of the outer firewall which forwards http connections to the Web server. A process on an internal host retrieves customer order information from the Web server in a timely manner and erases that information, except for logs, from the DMZ Web server.

The DMZ Web server also runs SSH services on the server for system administration duties only. The SSH server is configured so that it only accepts connects from the trusted internal admin host. Any customer data collected is encrypted and stored elsewhere on the server using public key encryption. An SSH connection is used to download that data to an internal server for order processing. By using public key encryption only the public key would be stored on the Web server. This means that even if an attacker did compromise the DMZ Web server, she would not be able to decrypt the data because she would not have the private key needed for the decryption. This is an application of the principles of least privilege, of separation of privilege and of fail-safe defaults.

DMZ DNS Server

The DMZ DNS host contains directory name service information about those hosts that the DMZ server must know. It contains entries for the following:

1. DMZ mail, WEB, and Log hosts
2. Internal trusted administrative host(s)
3. Outer Firewall
4. Inner Firewall

Note: The DNS server does not know the addresses of the internal mail servers. The inner firewall forwards mail to the appropriate mail server.

The DMZ DNS server only needs to update the address table if the address of the internal trusted admin host changes. The limited information in the DNS server reflects the principle of least privilege.
DMZ Log Server

The log server performs an administrative function. All DMZ machines have logging turned on. In the event of a compromise or an attempted compromised, these logs will be invaluable in assessing the method of attack, the damage or potential damage, and the best response.

Log Host in DMZ
1. all hosts have logging turned on
2. log to self and log server
3. log to disk and write once media
4. accept SSH connection from admin host only

Internal Network

The internal network is organized into a number of subnets. Each subnet must guard against unauthorized access to information as dictated by the security policy. The constraints on information flow dictate the arrangement of the network. The firewalls impose the confinement required at the interfaces. A graphic depiction of the internal network is given below:

Security Goal

Guard internal data from being stolen by outside attacker

Who is most likely to steal data? insider or outsider

Progressive Insurance Story
employee accessed foreclosure database to buy/sell real estate
Terminated!

Subnets guard against unauthorized access of information as dictated by policy

Firewalls may be
either proxy or filtering
implement access control matrix
Internal mail server must be able to communicate with hosts behind each subnet firewall.

Internal web server – development firewalls allow access

Trusted internal administrative machine
  only system admins
  only machine allowed access through inner firewall with SSH
  mail server & DNS server also access through inner firewall

DMZ servers only know about inner firewall address & admin machine

No direct communications with any internal machine

Only data written from DMZ is customer data which is encrypted, checked, and never executed.

Assurance

All of the defenses discussed depend on software that has been written defensively. If this trust is misplaced, the defensive mechanisms can be breached. This is another reason why the configuration of servers and firewalls is based extensively on the principle of separation of mechanisms. If one mechanisms fails, another may prevent the attacker from exploiting that failure.