

**WEL COME**

**in zone of**








**FIRE  
WARE**









# Content::

---

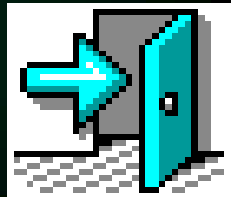
- ✓ INTRODUCTION 
- ✓ WHAT WE ARE TRYING TO PROTECT? 
- ✓ WHAT ARE YOU TRYING TO PROTECT AGAINST? 
- ✓ WHAT IS AN INTERNET FIREWALL? 
- ✓ HOW IT PROVIDE SECURITY? 





- 
- ✓ WHAT ARE THE TYPES OF FIREWALLS? 
  - ✓ WHAT CAN A FIREWALL DO? 
  - ✓ WHAT CAN'T A FIRE WALL DO? 
  - ✓ FIREWALL ARCHITECTURES 
  - ✓ FIREWALL DESIGN 
  - ✓ BIBLIOGRAPHY 

END




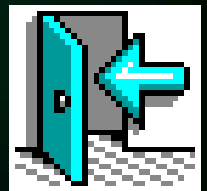


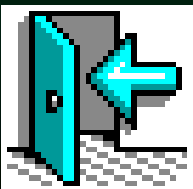
# INTRODUCTION

---

- ▼ In a building construct , a firewall is designed to keep a fire from spreading one part of the building to another.

A Internet firewall serves a similar purpose : it prevents the danger of Internet from spreading to your Internal network 






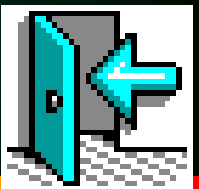


# WHAT IS A FIREWALL EXACTLY?

---

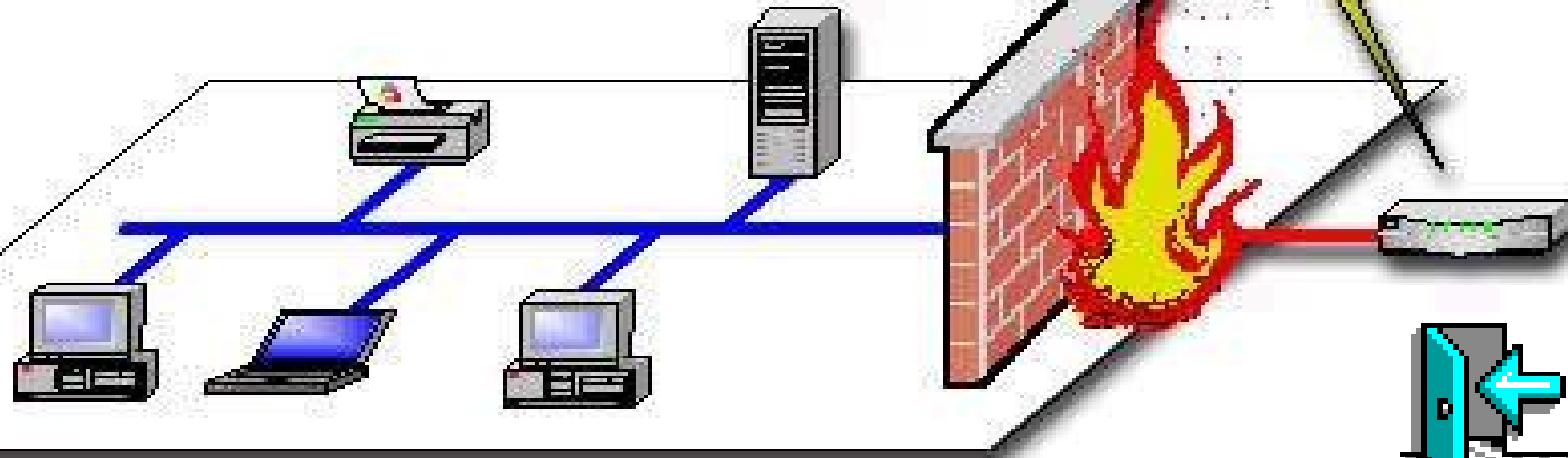
- ✓ A Firewall is simply a system designed to prevent unauthorized access to or from a private networks.

Firewalls can be implemented in both hardware and software, or the combination of both. 





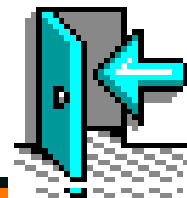
**HAKKER**



# ATTACK

Distributed denial of service (DDOS) attacks, which have been used recently to knock leading e-commerce sites offline, use multiple computers to send a flood of electronic traffic to the targeted Web site. That eventually overloads the computer network and renders it inaccessible.

Such electronic bombardments are not new, but the attackers have now planted software “tools” that can be activated remotely into hundreds, if not thousands, of computers around the world, exponentially increasing their ability to create mayhem.



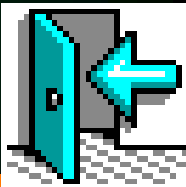




# WHAT ARE YOU TRYING TO PROTECT?

---

- ✦ YOUR DATA: the information you keep on the computers.
- ✦ YOUR RESOURCES: the computer themselves.
- ✦ YOUR REPUTATION.





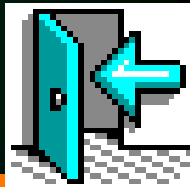
# WHAT ARE WE TRYING TO PROTECT AGAINST?

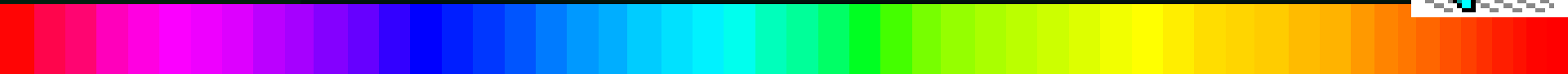
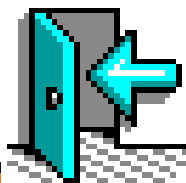
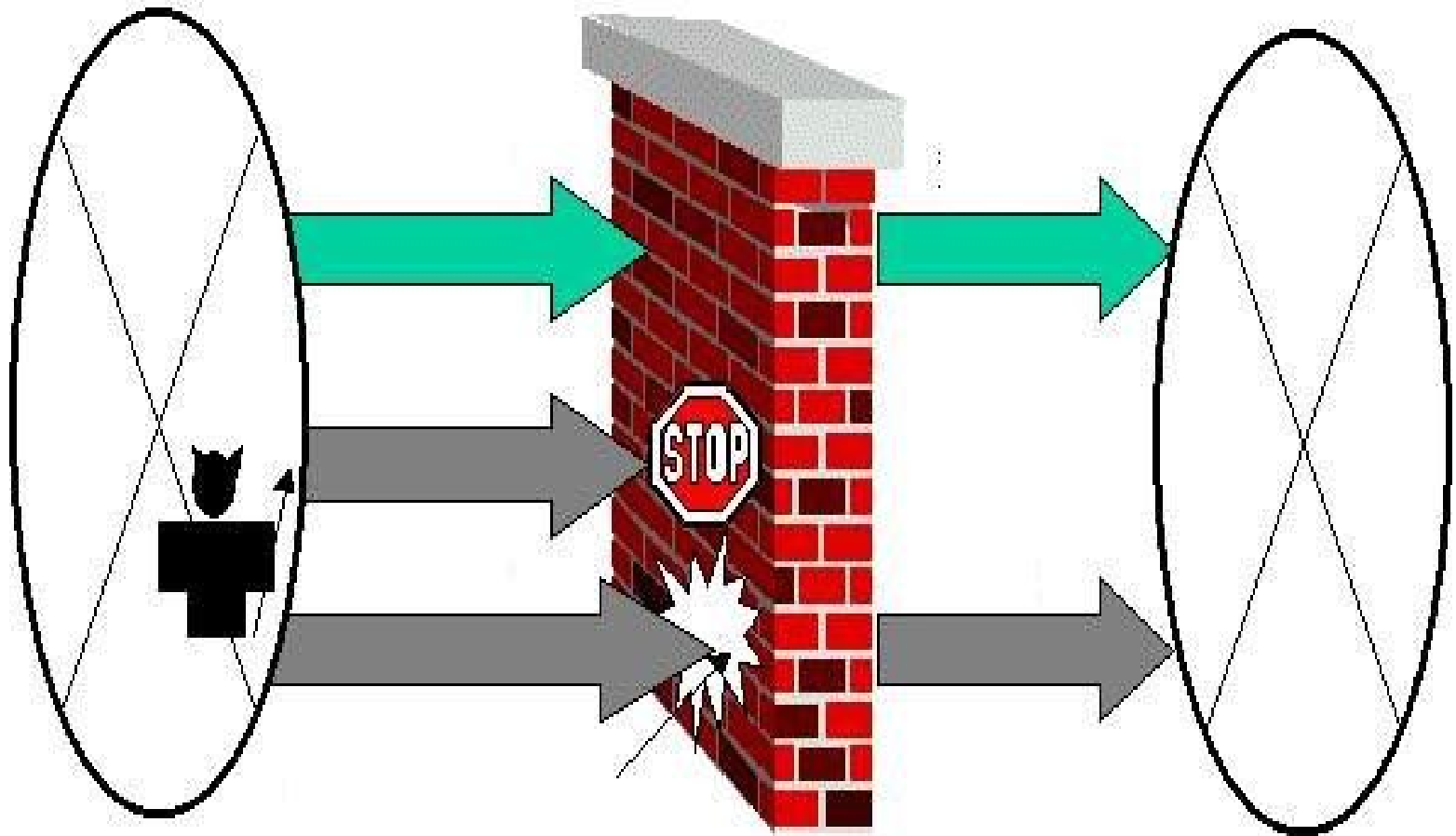
---

- ✓ All the thing which we have is to be protected against attacks.

Attacks are mainly categorized as:

1. Intrusion.
2. Denial of service ( DOS).
3. Information Theft.



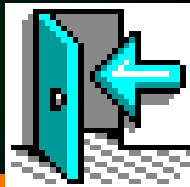




# WHAT CAN A FIREWALL DO?

Firewall can do a lot of for your site's security. In fact, some advantages of using firewalls are :

- ✓ A firewall is a focus for security decisions.
- ✓ A firewall can enforce a security policy.
- ✓ A firewall provide segmentation and isolation.
- ✓ A firewall limits your exposure.

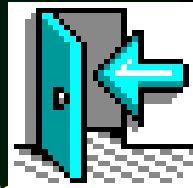




# WHAT CAN,T A FIREWALL DO?

Firewalls offer excellent protection against network threats ,but they are not a complete security solution

- ❖ Firewall can't protect you against malicious Insiders
- ❖ Detecting a virus in a random packet of data passing through a firewall.
- ❖ A firewall can't protect you against connections that don't go through it.
- ❖ A firewall can't set itself up correctly.
- ❖ A firewall can't protect against completely new threats.





T

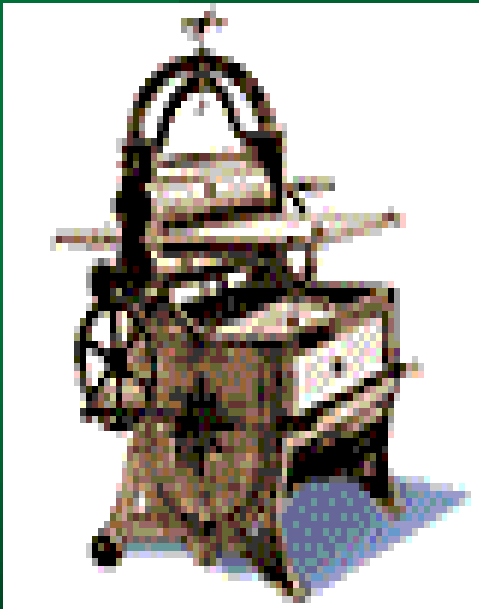
H

A

N

K



YOU

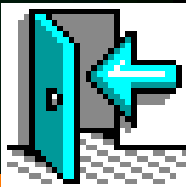


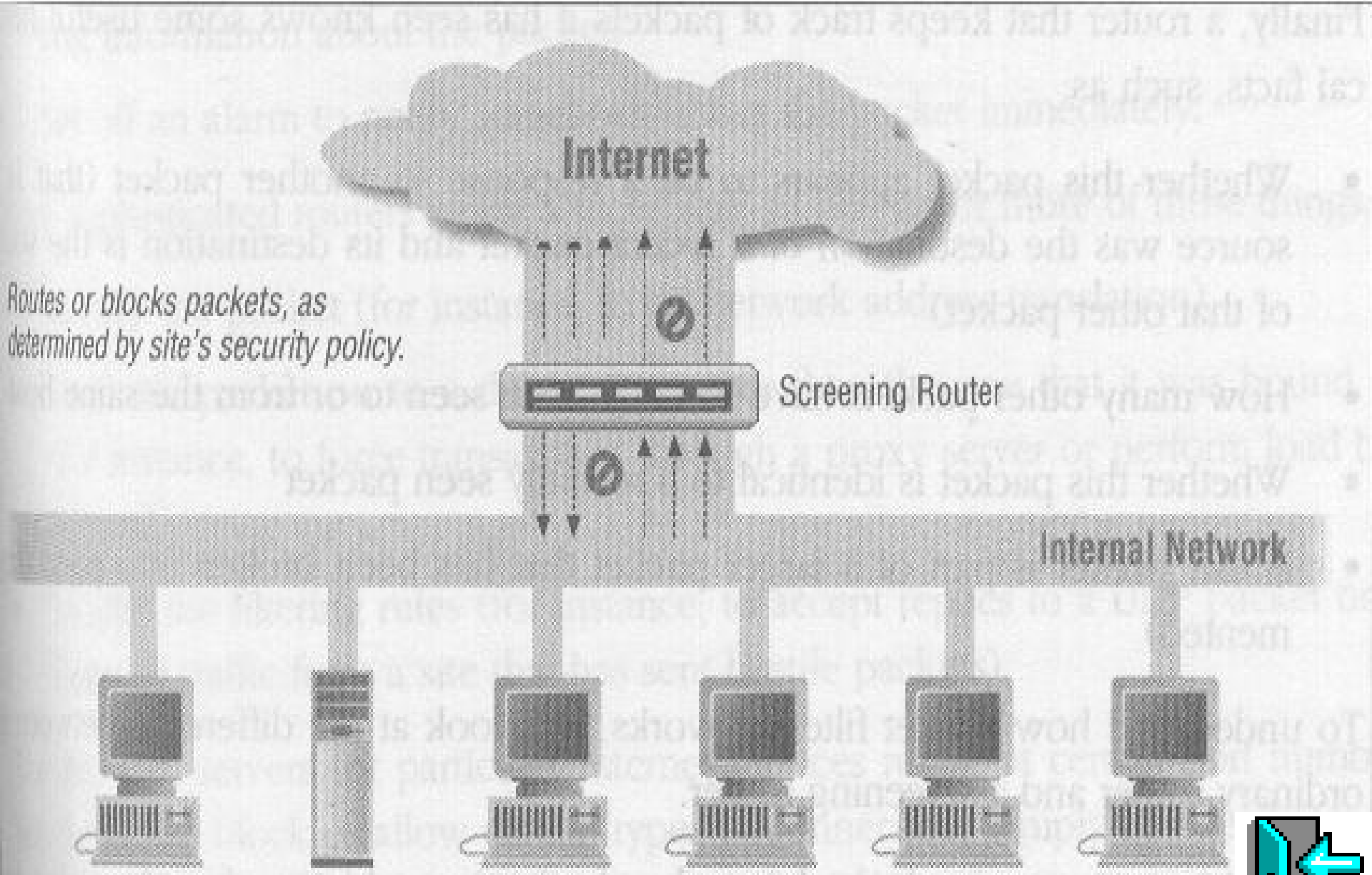


# TYPES OF FIREWALLS?

There are three kinds of firewalls. You can think of them as being like the ways you can screen phone calls.

- ✓ Packet filter firewalls. 
- ✓ Proxy firewalls. 
- ✓ Personal software firewalls.





*Routes or blocks packets, as determined by site's security policy.*

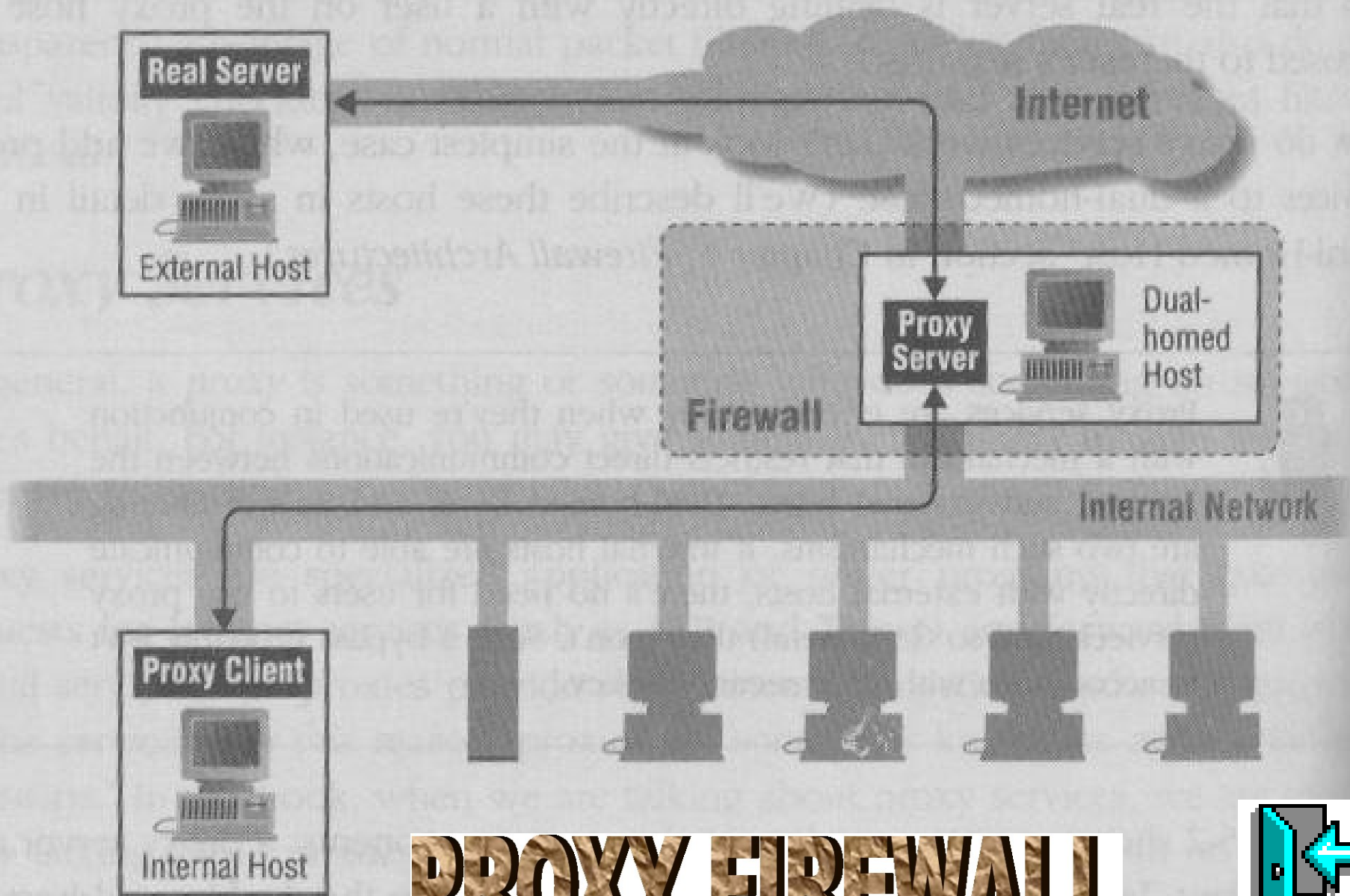
Screening Router

Internal Network

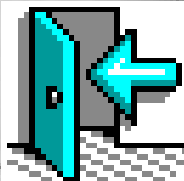
# Packet Filtering Firewall





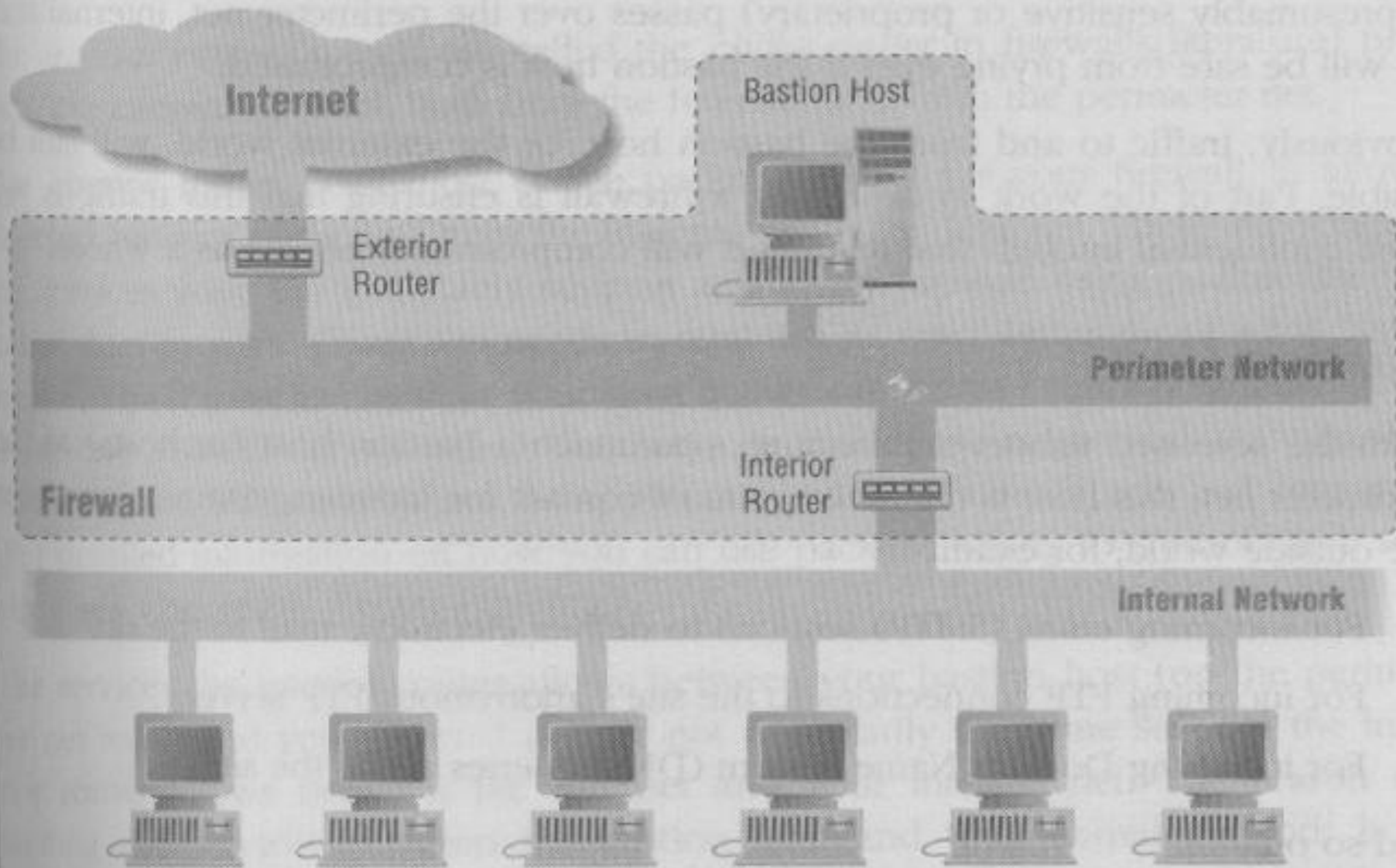


# PROXY FIREWALL

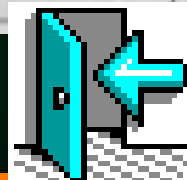




- ✓ Proxies are like a secretary in an office. The secretary takes the call, finds out who is calling and why, and decides what to do. Based on the caller's identity and reasons, they might transfer the call to the appropriate person, take a message (which would be like logging the call), or choose to ignore the call (if it was a wrong number, or a caller from a competitor).



# SCREENED HOST ARCHITECTURE





# FIREWALL ARCHITECTURES

Firewall architectures are categorized as:

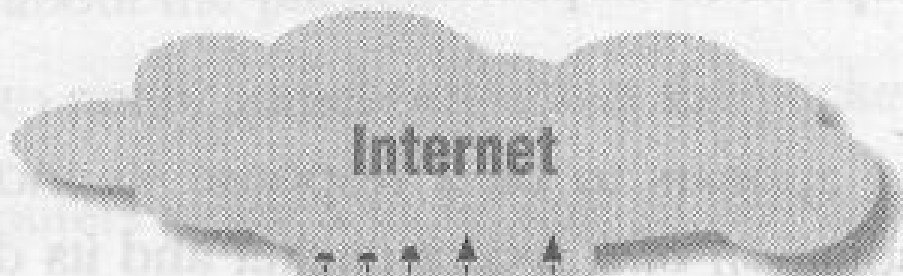
\* Single-Box Architectures.

\* Screening Router. 

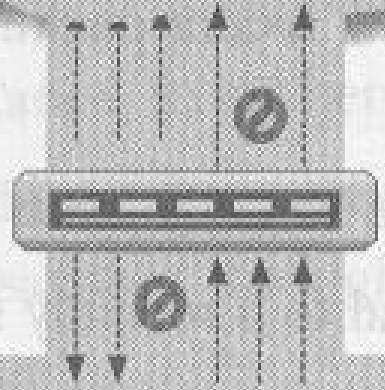
\* Dual-Homed Host. 

\* Screened Host Architectures 

*Routes or blocks packets, as determined by site's security policy.*

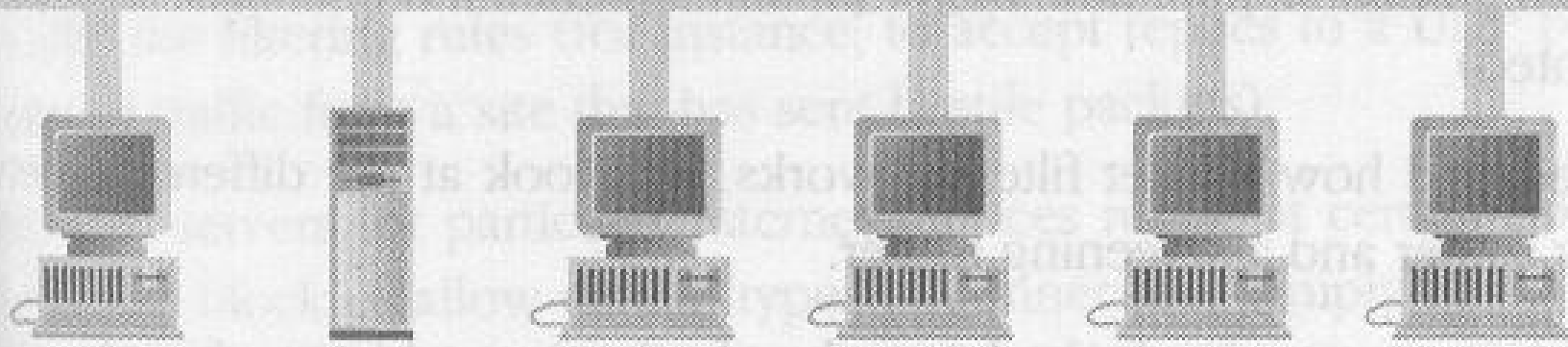


Internet

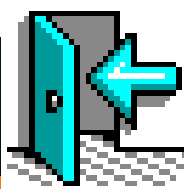


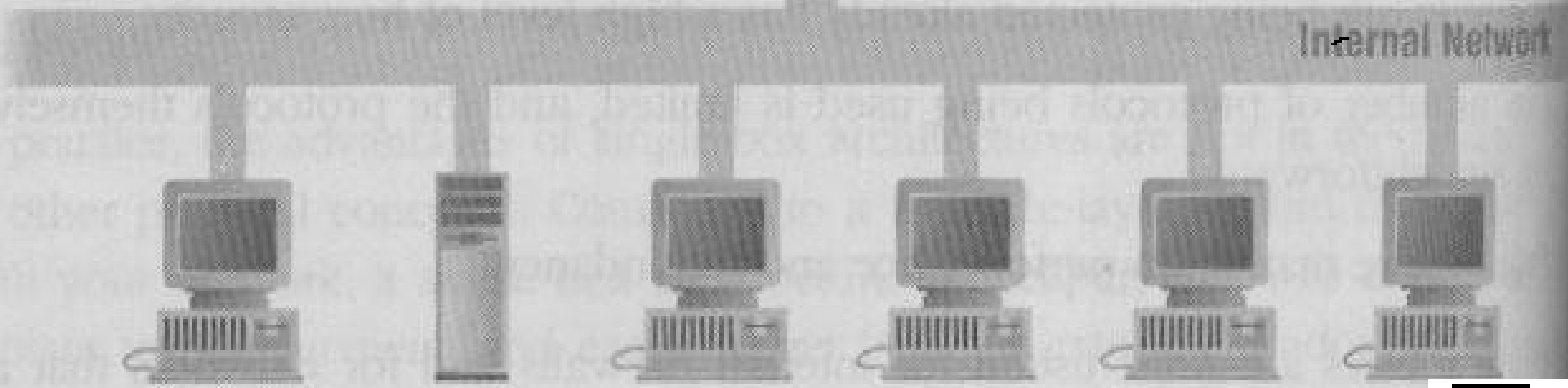
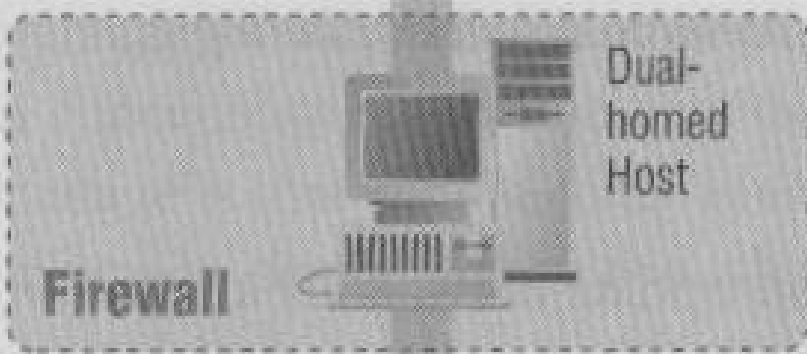
Screening Router

Internal Network

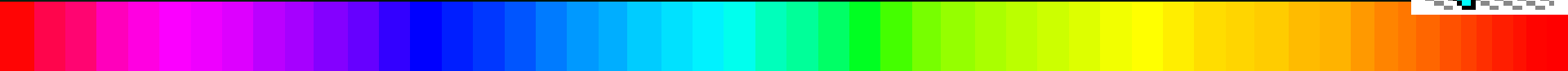
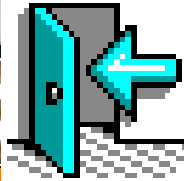


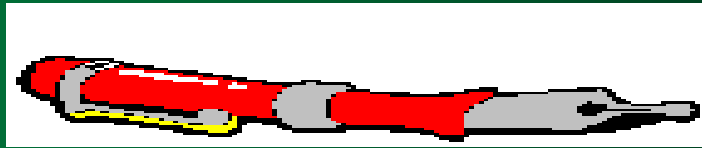
# SCREENING ROUTER ARCHITECTURE





# DUAL-HOMED HOST ARCHITECTURE





# BIBLIOGRAPHY

- \* Building Internet Firewalls

Zwiecky, Cooper & Chapman

- \* Data Communication And Networking

Behrouz A. Forouzan

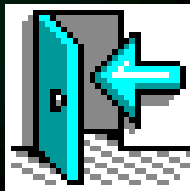
- \* Internet Security Protocols

Uyless Black

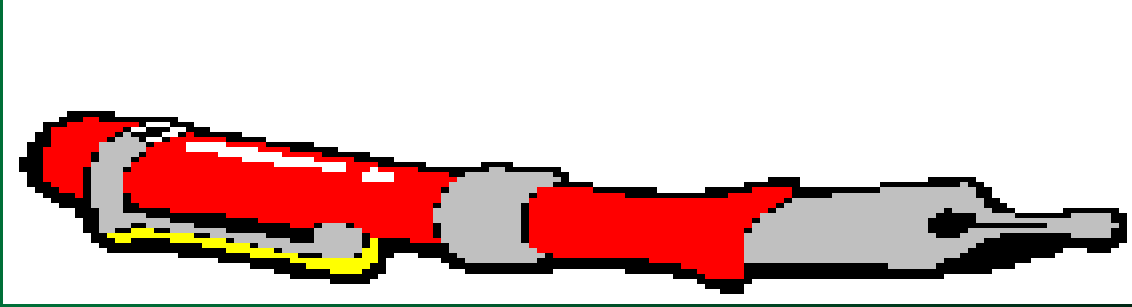
- \* [WWW.FIREWALL.CX](http://WWW.FIREWALL.CX)

- \* [WWW.OREILLY.COM](http://WWW.OREILLY.COM)

- \* [WWW.VULCAN.FE.ISTATE.EDU](http://WWW.VULCAN.FE.ISTATE.EDU)







\* Building Internet Firewalls

Zwiecky, Cooper & Chapman

\* Data Communication And Networking

Behrouz A. Forouzan

\* Internet Security Protocols

Uyless Black

\* [WWW.FIREWALL.CX](http://WWW.FIREWALL.CX)

\* [WWW.OREILLY.COM](http://WWW.OREILLY.COM)

\* [WWW.VULCAN.EE.ISTATE.EDU](http://WWW.VULCAN.EE.ISTATE.EDU)






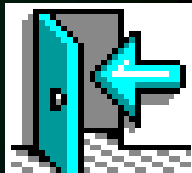




# FIREWALL DESIGN

When you design a firewall, you go through the basic outline as:

- ▼ Define your needs. 
- ▼ Evaluate the available products. 
- ▼ Figure out , How to assemble the products in to working firewall? 

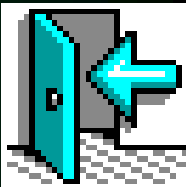




# DEFINE YOUR NEED

What will Actually do for you?

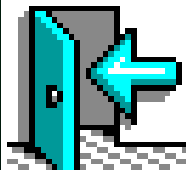
- ▼ Decide service need to offer?
- ▼ Decide security.
- ▼ Decide usage.
- ▼ Decide reliability





# WHAT ARE YOUR CONSTRAINTS?

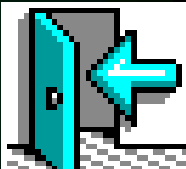
- ▼ Your budget.
- ▼ Personal availability.
- ▼ Environment.





# EVALUATE THE AVAILABLE PRODUCTS

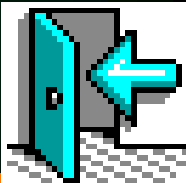
- ✓ Scalability
- ✓ Reliability and Redundancy.
- ✓ Price.
- ✓ Management and Configuration.





# PUT EVERYTHING TOGETHER

- ▼ Where will logs go, and how?
- ▼ How will you back up the system?
- ▼ What support services does the system require?
- ▼ How will you access the machines?
- ▼ Where will routine reports go, and how?





# Business Concept

- ✓ Summarize key technology, concept or strategy on which your business is based



# Competition

- ✓ Summarize competition
- ✓ Outline your company's competitive advantage



# Goals & Objectives

- ✓ Five-year goals
  - State specific measurable objectives
  - State market share objectives
  - State revenue/profitability objectives





# Financial Plan

- ✓ High-level financial plan that defines financial model, pricing assumptions, and reviews yearly expected sales and profits for the next three years.
- ✓ Use several slides to cover this material appropriately.



# Resource Requirements

- ✓ Technology requirements
- ✓ Personnel requirements
- ✓ Resource requirements
  - Financial, distribution, promotion, etc.
- ✓ External requirements
  - Products/services/technology required to be purchased outside company



# Risks & Rewards

## ✓ Risks

- Summarize risks of proposed project

## ✓ Addressing risk

- Summarize how risks will be addressed

## ✓ Rewards

- Estimate expected pay-off, particularly if seeking funding



# Key Issues

## ▼ Near term

- Isolate key decisions and issues that need resolution

## ▼ Long term

- Isolate issues needing long-term resolution
- State consequences of decision postponement

## ▼ If you are seeking funding, state specifics

