Firewalls and Proxy Servers

By Stephen Hewitt
Speedware Corp
9999 Cavendish Blvd.
St. Laurent, Quebec
Canada
Ph. 800 361 6782
Fax 514 747 3320
shewitt@speedware.com

Firewalls and Proxy Servers

Who's Protecting You?

By Stephen Hewitt

What Are We Trying To Protect

- Data
- Internal Systems
- DOS Attacks
- Internet Access
- Users From Themselves

How Are We Going To Protect It

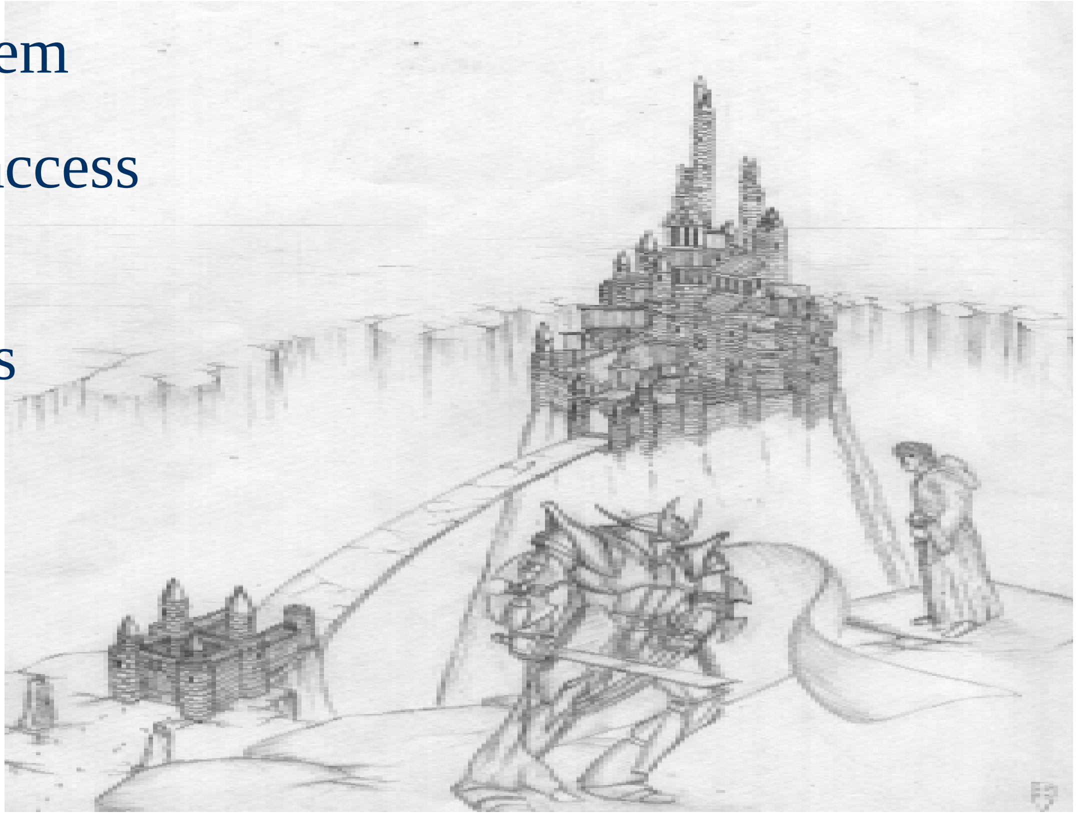
- No Web Presence
- No Internet Access for anyone
- No email for anyone
- No FTP for anyone

OR

Firewalls and Proxy Servers

What Is A Firewall

- Perimeter Defense System
- Prevents unauthorized access to internal systems
- Any device that controls Network Access either internally or externally



Types of Firewalls

- Screening Routers
- Proxy Server Gateways
- Stateful Inspection

Screening Routers

- Looks at information related to IP’s (Network Layer) and type of connection (Transport Layer)
- Applies filters based on information
- Can be stand alone or a dual honed machine

Proxy Server Gateways

- Circuit Level Gateway
  - alter IP address’s
  - Usually entails two network cards
- Application Level Gateway
  - control access to FTP, Telnet etc by use of Ports

Stateful Inspection

- Gets around biggest disadvantage of Proxy Servers by “remembering” requests
- Stores information on original request and remembers it
- If it receives the same request again does not have to analyze every packet

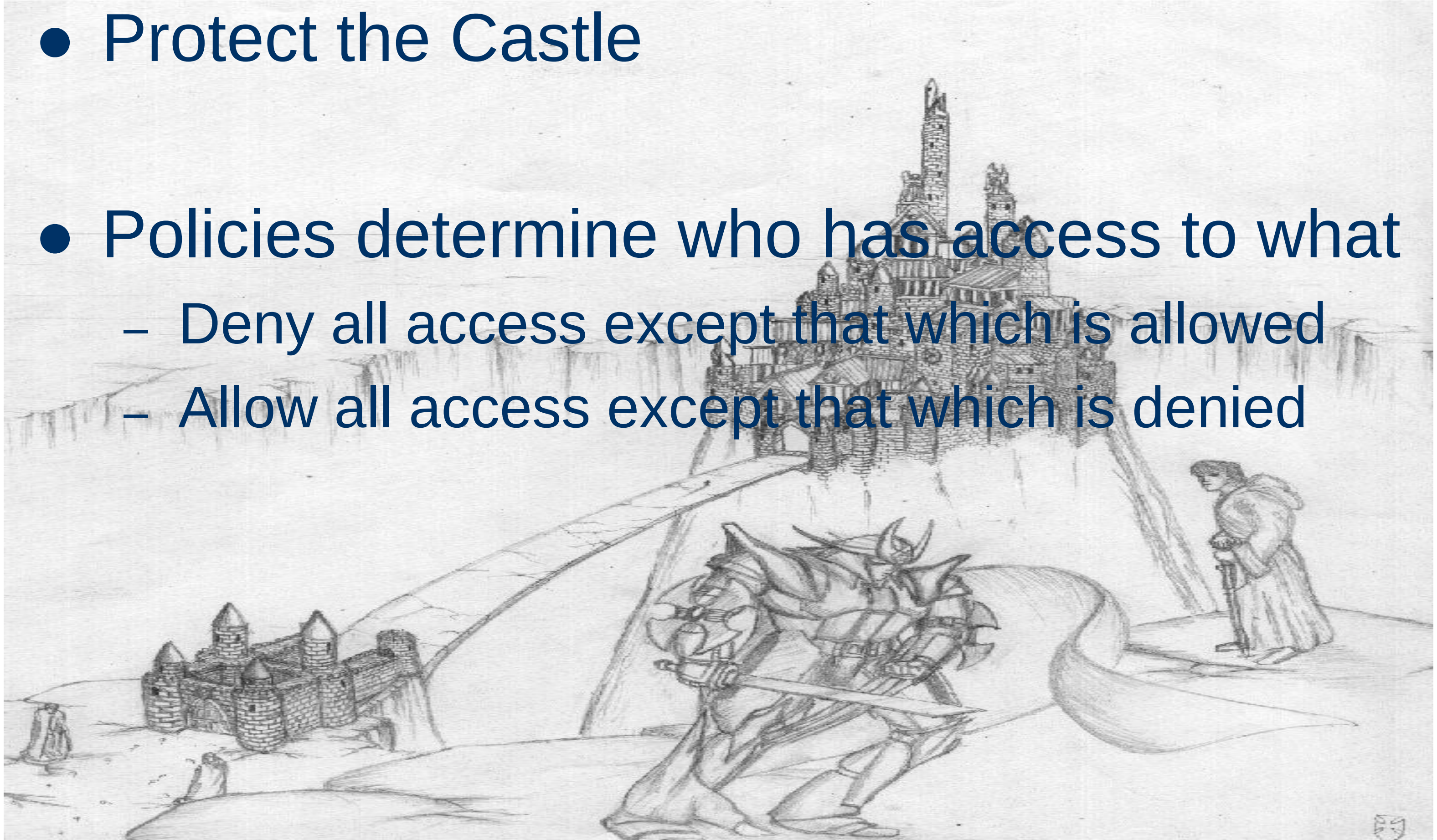
What Is A Proxy Server

- Component of Firewall
- Controls access to the Network from the Internet
- Controls access to the Internet from the Network
- Allows or Prevents access to Applications

Ports

- Can be used to define routes through a firewall
- Is part of a packet
- Examples
  - FTP – 20 and 21
  - HTTP 80
  - Telnet - 23
  - SMTP - 25
  - Database Access – 4000

How Does It All Work???



- Protect the Castle
- Policies determine who has access to what
  - Deny all access except that which is allowed
  - Allow all access except that which is denied

Deny All Access

- Start by denying access to everything
- Allow access to systems as they become necessary

Allow Access to Everything

- Star by allowing access to everything
- Restrict access as it becomes necessary

Conclusion Part I

- What are you trying to protect against?
- What sort of access to your systems do you need?
- Cost

Conclusion Part II

Give your System the peace of mind it deserves!