SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

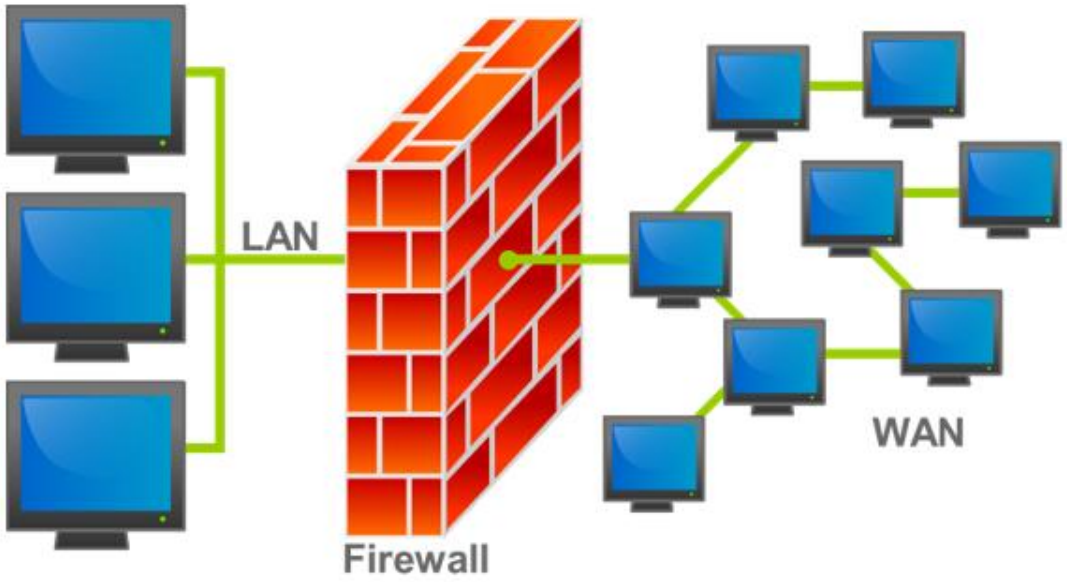
III YEAR / VI SEMESTER

Unit 5: CYBER SECURITY SAFEGUARDS AND SECURITY SERVICES

Topic : Firewalls

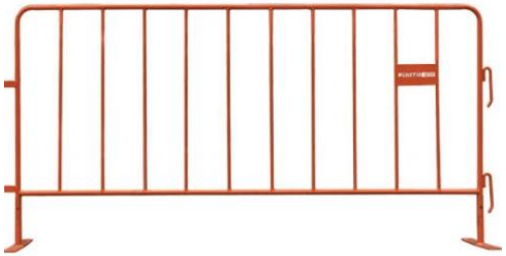
Firewalls

Firewall

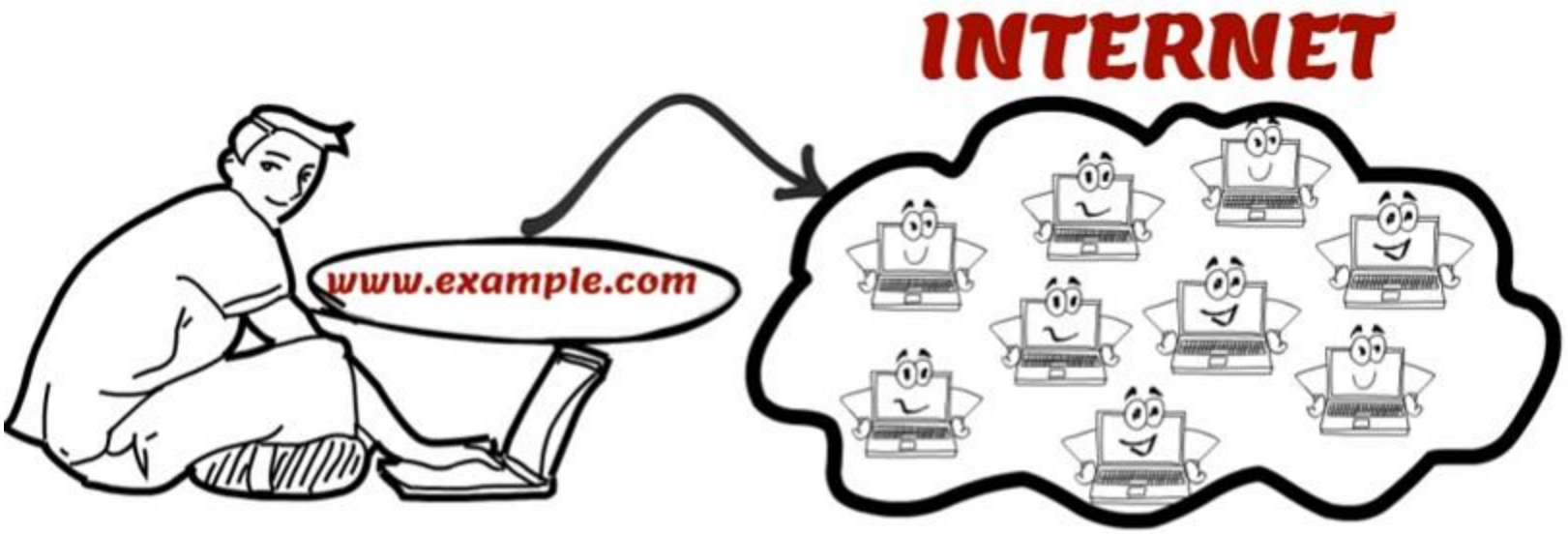


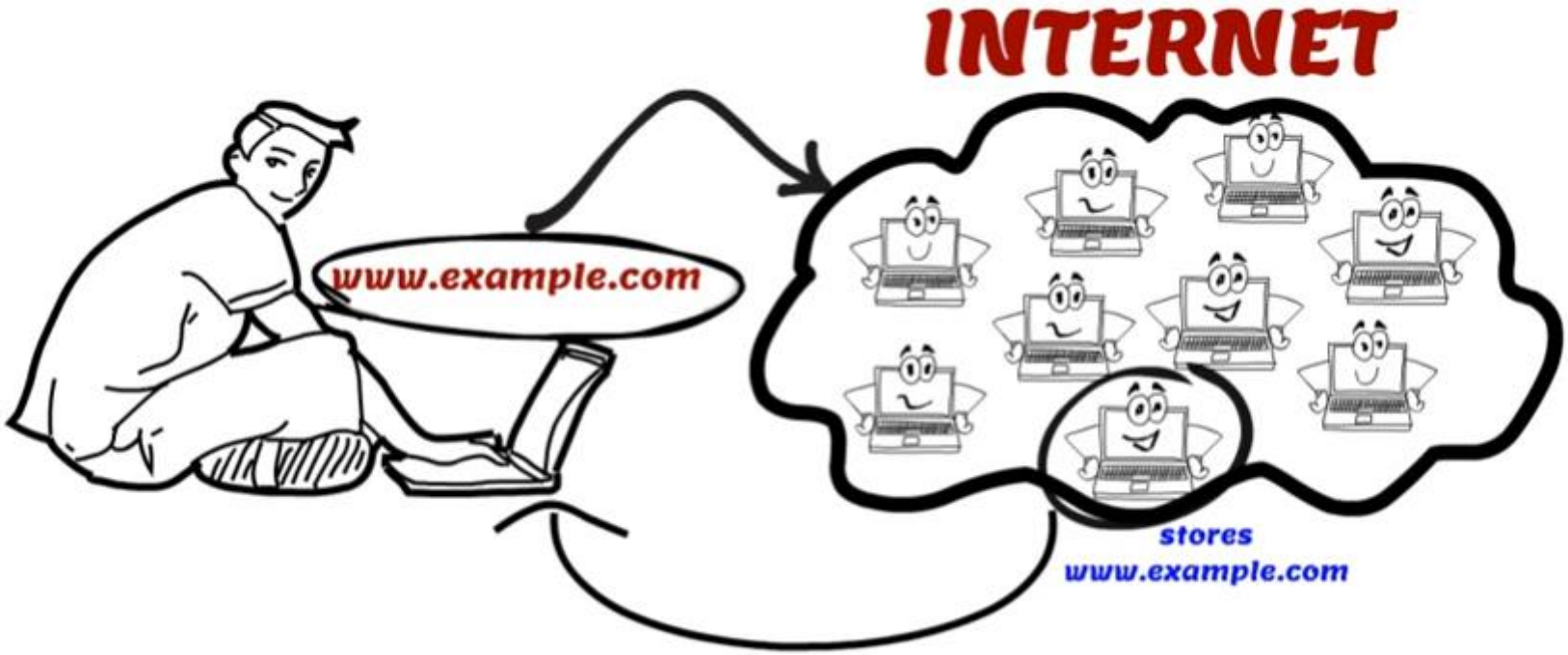
Firewall - Definition

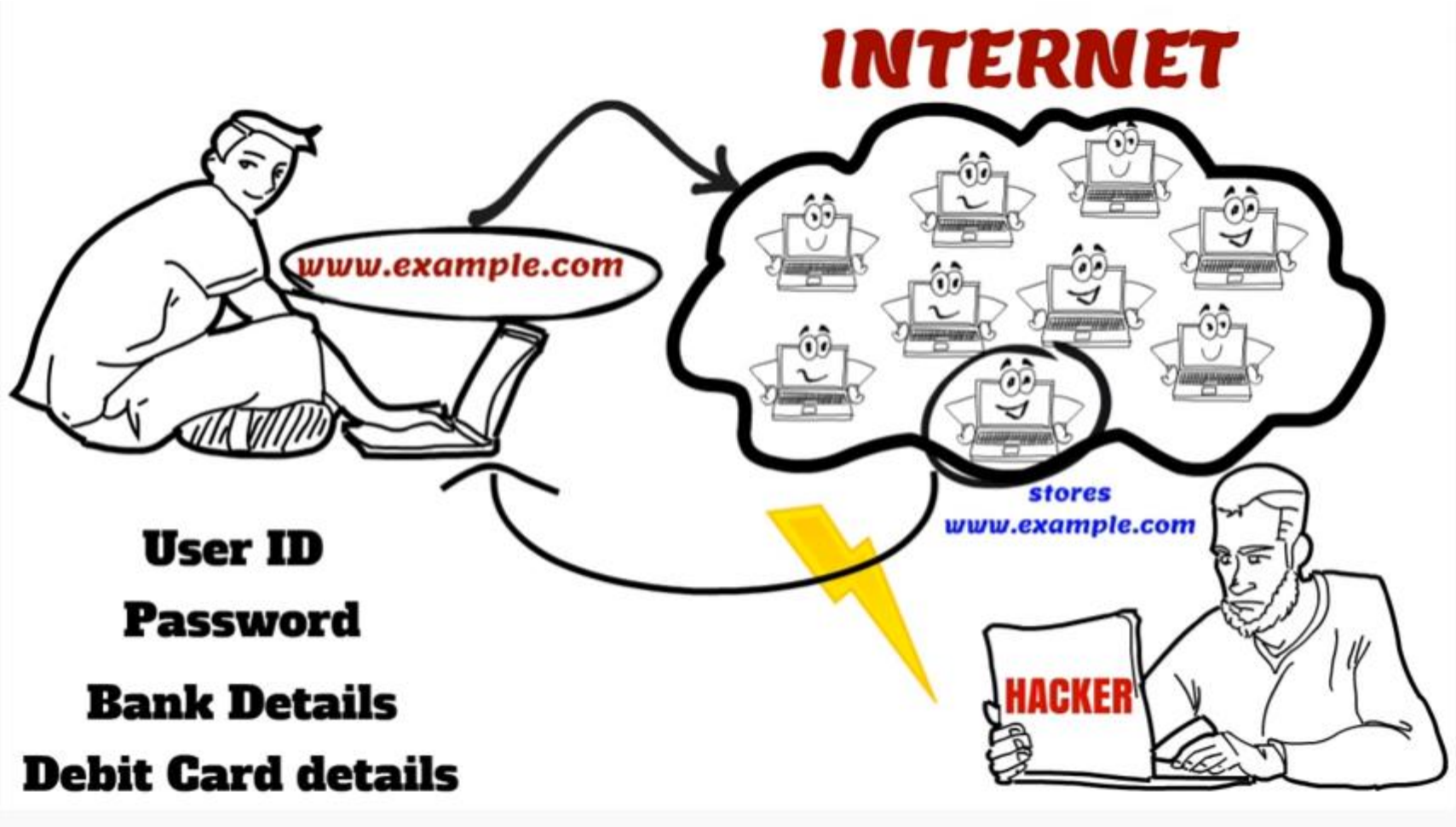
- Forms a **Barrier** through which the traffic going in each direction must pass
- **Authorize** which traffic to pass in each direction
- Firewalls can be an **effective means of protecting** a local system or network of systems from network-based security threats while at the same time **affording access to the outside world** via wide area networks and the Internet.

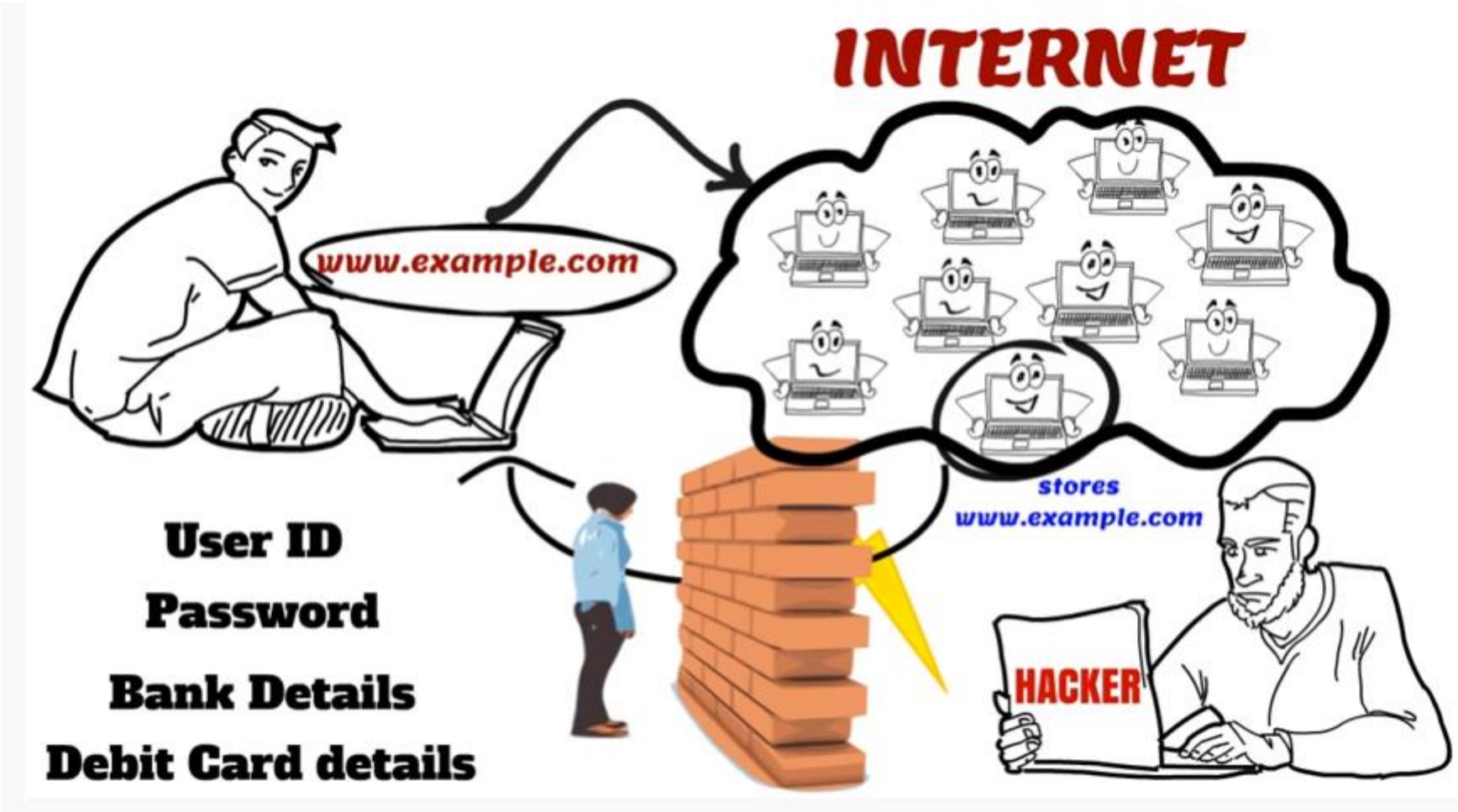


How Firewall Works?



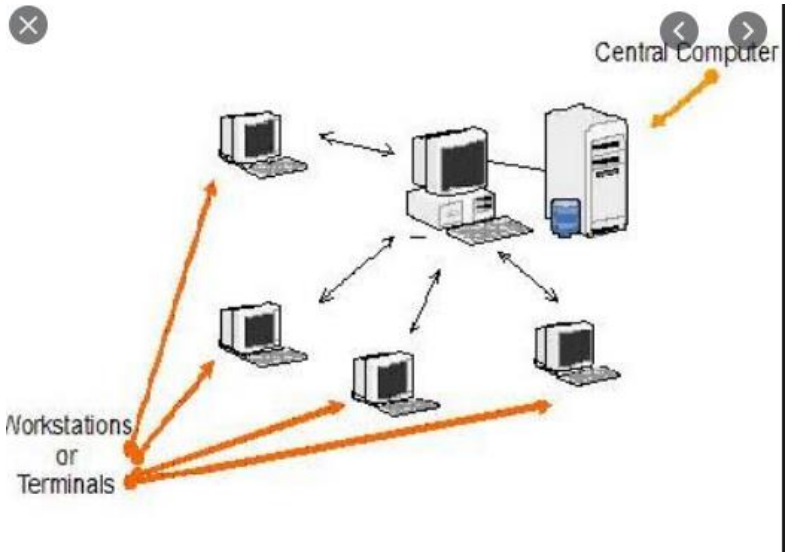

INTERNET
www.example.com
stores
www.example.com


INTERNET
www.example.com
stores
www.example.com
User ID
Password
Bank Details
Debit Card details
HACKER


INTERNET
www.example.com
stores
www.example.com
User ID
Password
Bank Details
Debit Card details
HACKER

Need for Firewall

- Notable Developments
  - Centralized data processing system
  - LAN
  - Premises Network
  - Internet Connectivity
  - Enterprise-wide network



Firewall Design Goals

- Enforcement of security policies
  - All traffic from inside to outside, and vice versa, must pass through the firewall.
  - Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- Dependable
  - The firewall itself is immune to penetration

General techniques

Control Access and enforce site security policy

- Service Control
- Direction Control
- User Control
- Behavior Control

Scope and Limitations

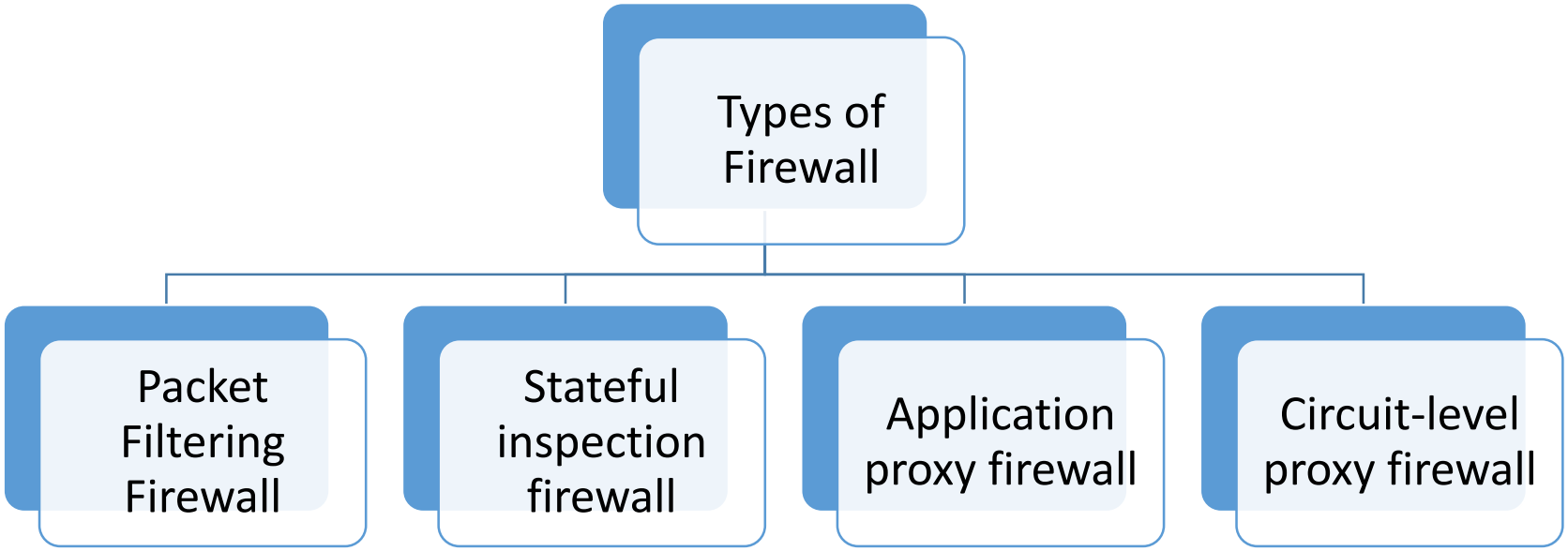
Scope

- Single Choke Point
- Monitor Security – related threats
- Convenient Platform
- Platform for IPSec

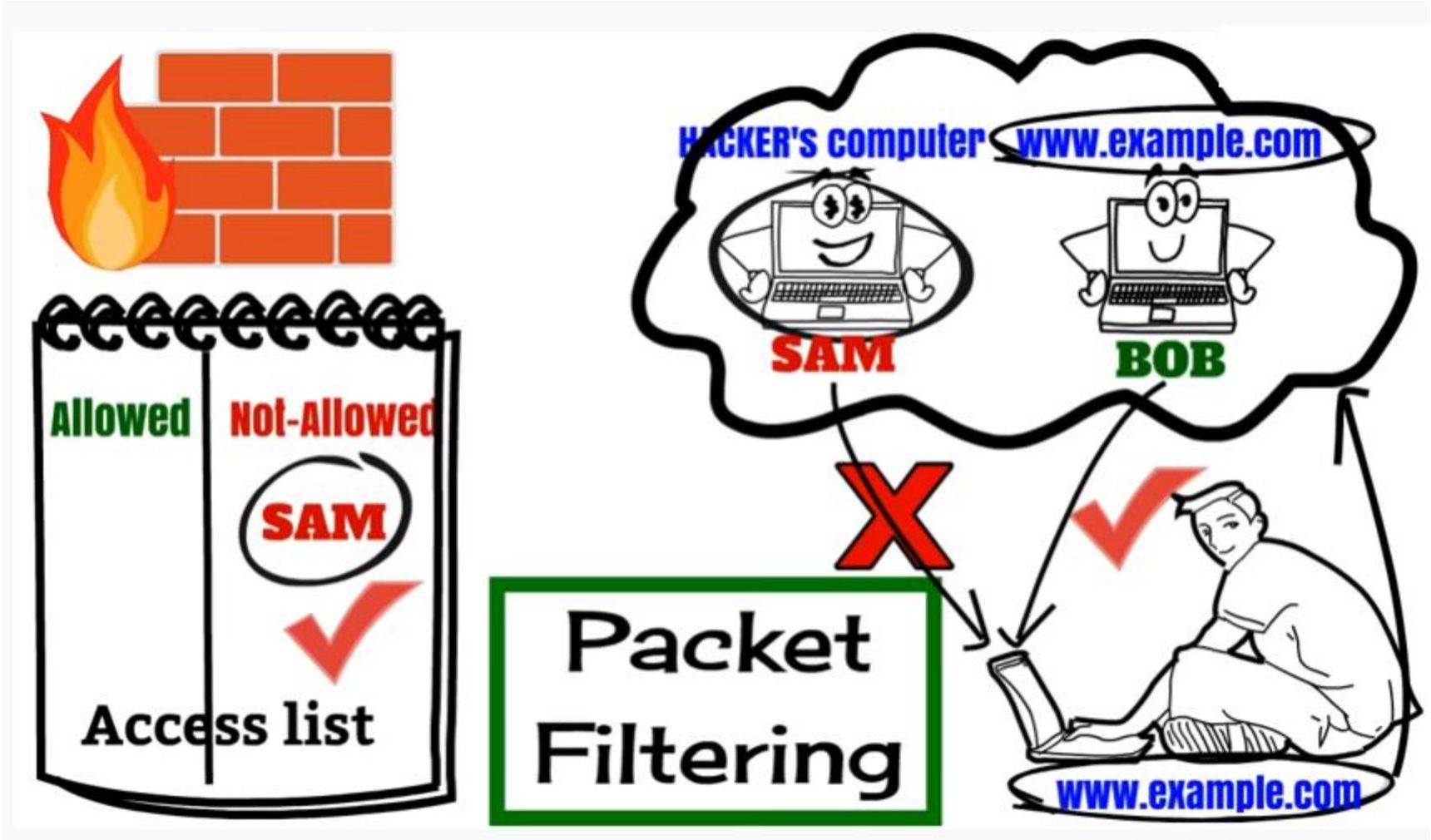
Limitations

- Cannot protect against attacks that bypass the firewall
- May not protect fully against internal threats
- improperly secured wireless LAN
- Portable devices – Affect when used internally

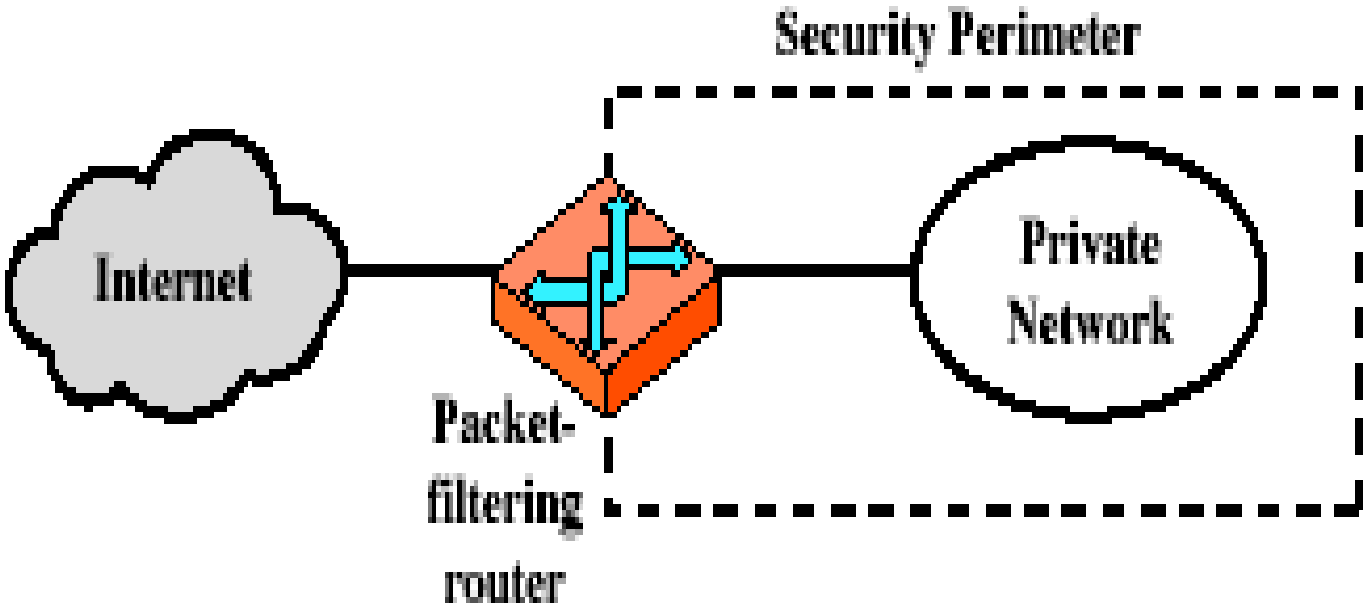
Types of Firewall



Packet Filtering Firewall



Firewalls – Packet Filters



(a) Packet-filtering router

Firewalls – Packet Filters

- simplest of components
- foundation of any firewall system
- examine each IP packet (no context) and permit or deny according to rules
- hence restrict access to services (ports)
- possible default policies
  - that not expressly permitted is prohibited
  - that not expressly prohibited is permitted

Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

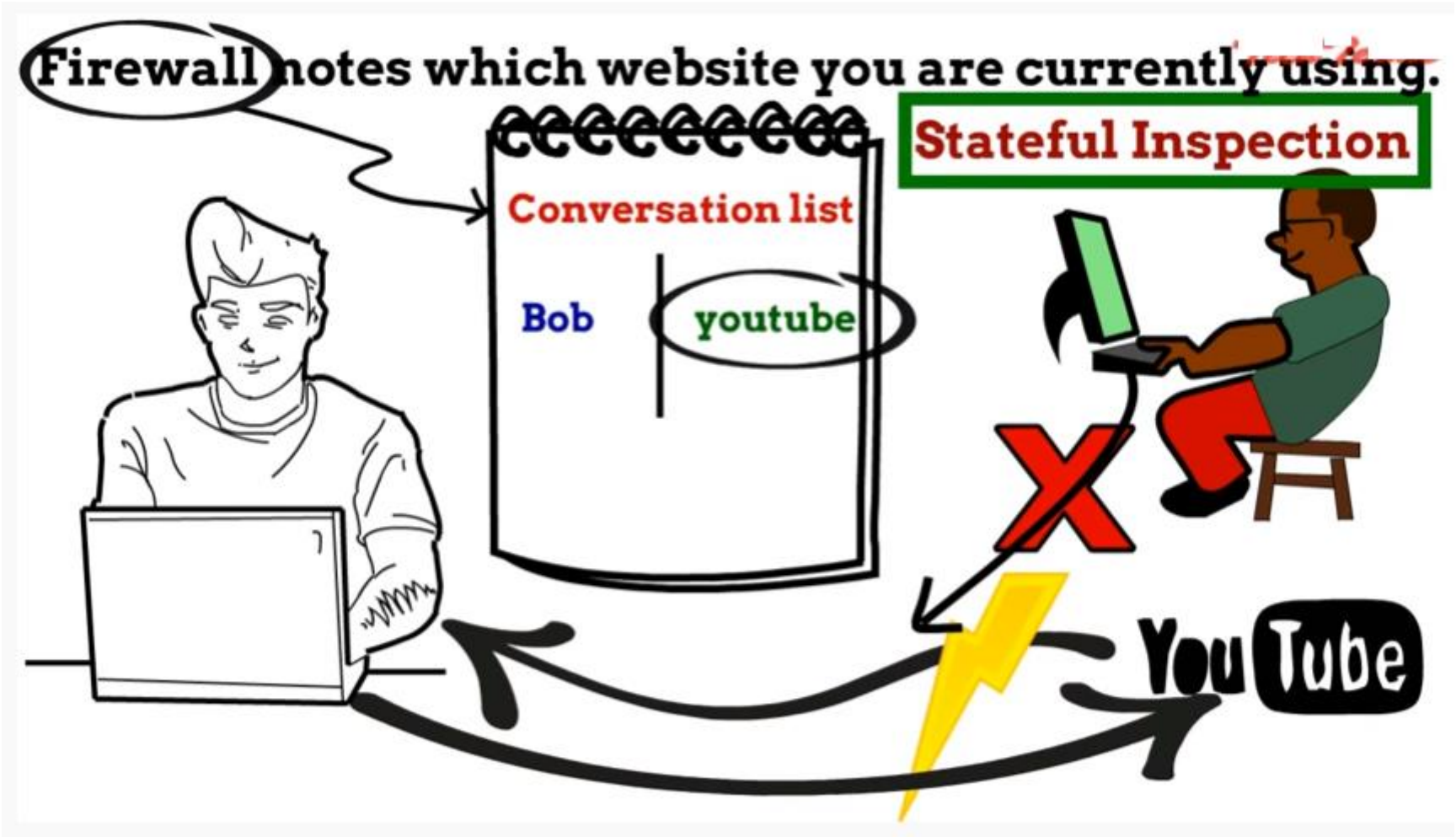
Advantage and Disadvantages

- Advantage
  - Simplicity
- Disadvantages
  - Do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions
  - The logging functionality present in packet filter firewalls is limited.
  - Do not support advanced user authentication schemes.
  - Vulnerable to attacks
  - Small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations.

Attacks on Packet Filters

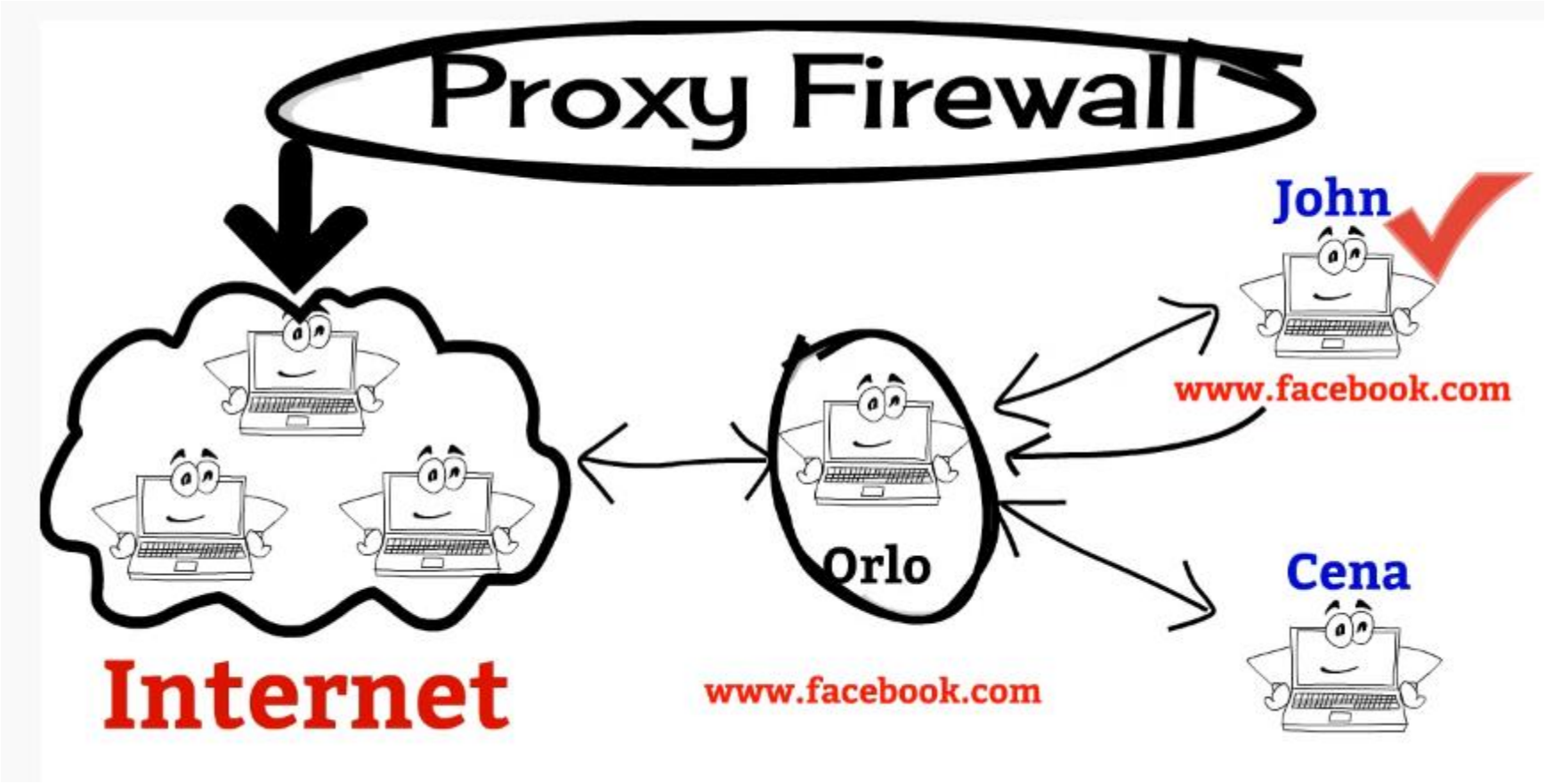
- IP address spoofing
  - fake source address to be trusted
  - add filters on router to block
- source routing attacks
  - attacker sets a route other than default
  - block source routed packets
- tiny fragment attacks
  - split header info over several tiny packets
  - either discard or reassemble before check

Stateful Inspection Firewall



- examine each IP packet in context
  - keeps tracks of client-server sessions
  - checks each packet validly belongs to one
- better able to detect bogus packets out of context

Application Level Gateway (or Proxy)



- use an application specific gateway / proxy
- has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic
  - custom services generally not supported

Advantages and Disadvantages

- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)

Firewalls - Circuit Level Gateway

- relays two TCP connections
- imposes security by limiting which such connections are allowed
- once created usually relays traffic without examining contents
- typically used when trust internal users by allowing general outbound connections
- SOCKS commonly used for this

Thank you