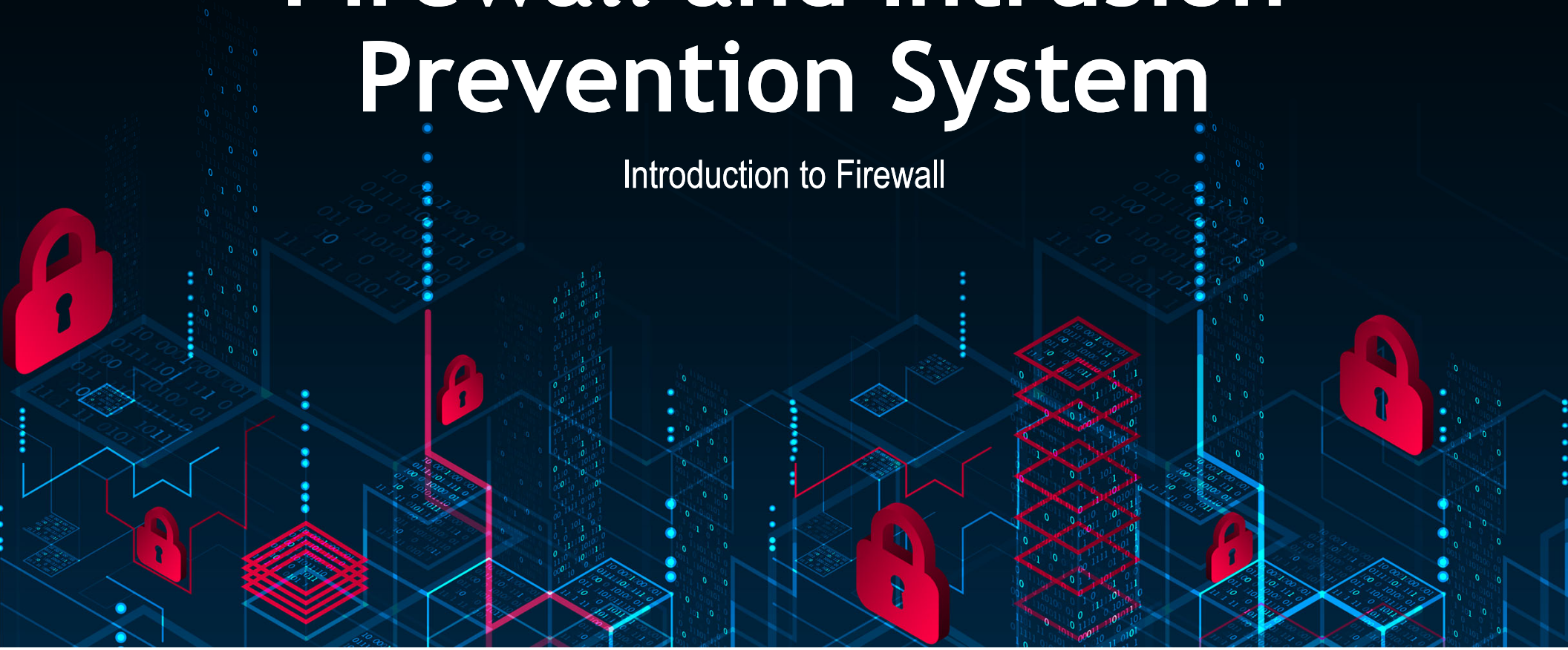
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Firewall and Intrusion Prevention System

Introduction to Firewall

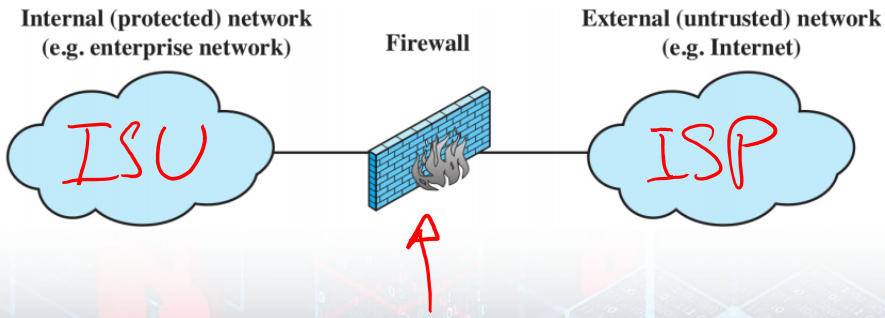


Video Summary

- Why we need Firewalls?
- Firewall Characteristics
- Capabilities and Limitations
- Types of Firewall
- TCP/IP Headers

The Need for Firewalls

- Internet connectivity is essential
  - However it creates a threat
- Effective means of protecting LANs
- Inserted between the premises network and the Internet to establish a controlled link
  - Can be a single computer system or a set of two or more systems working together
- Used as a perimeter defence
  - Single entry point to impose security and auditing (access control – malware… etc)
  - Insulates the internal systems from external networks

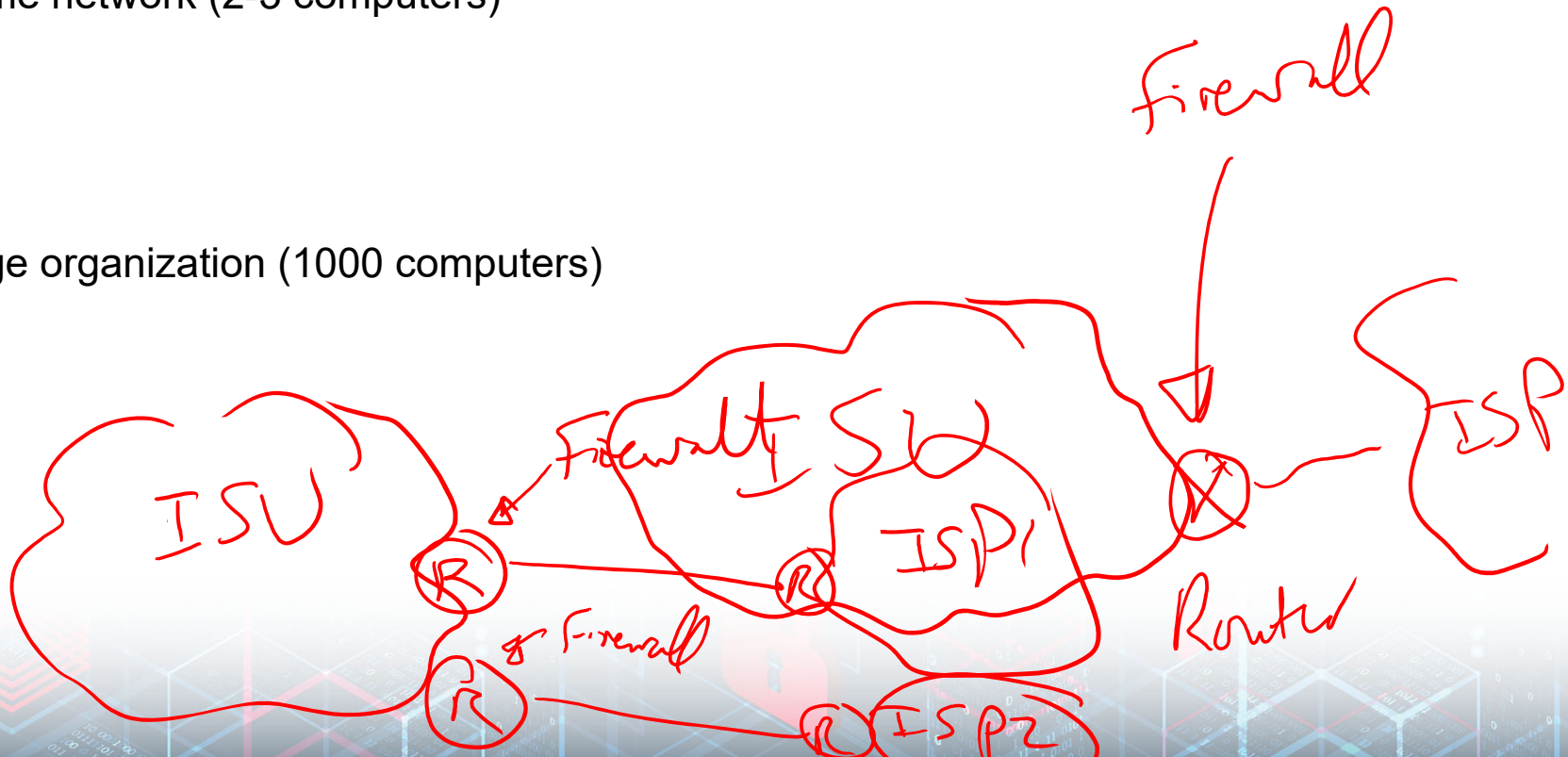


Location of the Firewall

- If the firewall is a software.. Where we would install/run it?

1. For home network (2-3 computers)

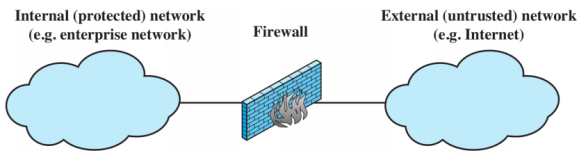
2. For large organization (1000 computers)



Firewalls Characteristics

Design Goals

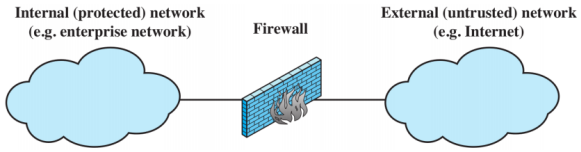
- All traffic from inside to outside must pass through the firewall
- Only authorised traffic as defined by the local security policy will be allowed to pass
- The firewall itself is immune to penetration



Prevent students from playing online games

Firewalls Characteristics

Design Goals



- All traffic from inside to outside must pass through the firewall
- Only authorised traffic as defined by the local security policy will be allowed to pass
- The firewall itself is immune to penetration

Prevent students from playing online games

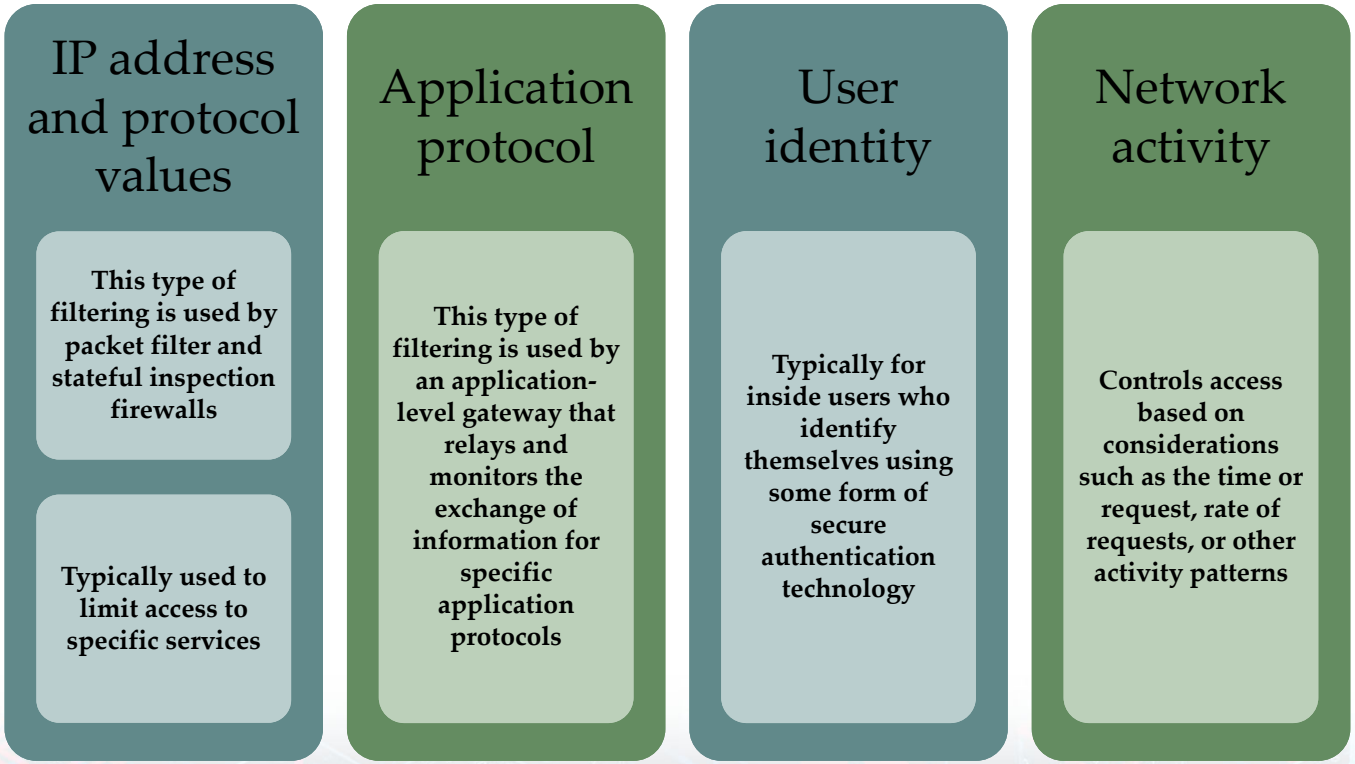
General Techniques

- Service control, e.g. filter based on IP address, port number
- Direction control, e.g. to internal LAN, to external Internet (Block Facebook vs Block malware)
- User control, e.g. student vs faculty
- Behaviour control, e.g. filter email with spam

online Games → faculty

Firewalls Characteristics

- Characteristics that a firewall access policy could use to filter traffic include:



Capabilities and Limitations

Capabilities

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related

Limitations

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Improperly secured wireless LAN can be accessed from outside the organisation (3G or 4G internet access)
- Laptop, phone, or USB drive may be infected outside the corporate network then used internally

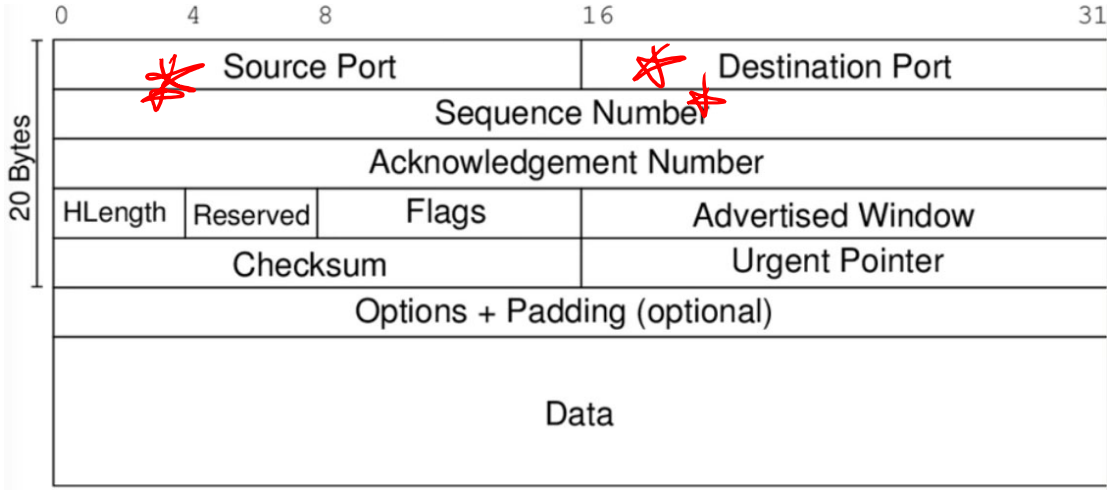
Types of Firewalls

- **Packet Filtering** accepts/rejects packets based on protocol headers
- **Stateful Packet Inspection** adds state information on what happened previously to packet filtering firewall
- **Application Proxy** relay for application traffic
- **Circuit-level Proxy** relay for transport connections

  - Normally a firewall is implemented on a router
  - That router may perform other (non-)security functions, e.g. VPN end-point, accounting, address and port translation (NAT)

SMY[C1

Protocol Header (TCP)



Port Number (what application)

Webserver (HTTP): 80

HTTPS: 443

Email (SMTP): 25

SSH: 22

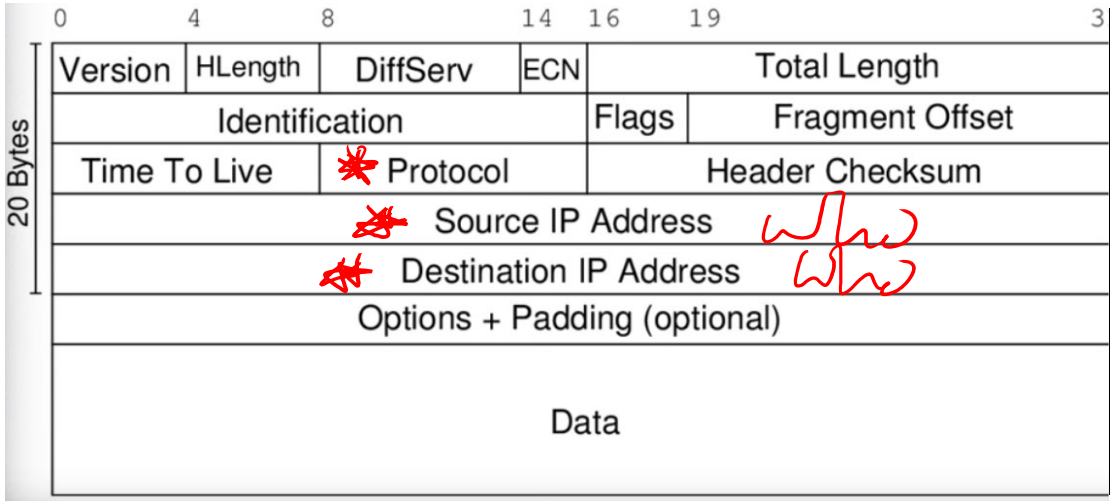
TelNet: 23

Remember these numbers!

Slide 10

SMY[C1 Selim, Mohamed Y [E CPE], 10/28/2019

Protocol Header (IP)



Protocol Number

TCP: 6
UDP: 17
ICMP: 1 → Ping

Remember these numbers!

Video Summary

- Why we need Firewalls?
- Firewall Characteristics
- Capabilities and Limitations
- Types of Firewall
- TCP/IP Headers