Network Design and Organisation

Josh Wilcox (jw14g24@soton.ac.uk)

March 4, 2025

Contents

1 Internet

- Global public network that connects worldwide devices uses standardised protocols
- Connects multiple smaller networks in one huge network
- Accessible to anyone with an internet connection

1.1 Security Risks

- Lack of data control
- Privacy concerns
- Vulnerable to hacking and malware

2 Intranet

- A private network restricted to the employees of an organisation
- Used for sharing info, resources, and tools *within* the organisation
- Accessible to only authorised people
- Isolated from public internet threats:
  - Uses firewalls and **VPNs**

3 Extranet

- A private network that **extends** certain service or access to external partners, clients or suppliers
- Accessible to external parties with restricted permissions
- Often use for collaboration between organisations

4 Comparison Table

	Internet	**Intranet**	**Extranet**
Access Users	Public	Private (Employees Only)	Private (With External Partners)
Connection Type	Public	Private	Private with External Access
Purpose	Global Connectivity	Internal Communication	External Collaboration
Access Control	Open to All, no access control	Broad access to **internal** users only	Restricted access to Partners
Security	Vulnerable to Threats	Secured with Firewalls	Secured with Firewalls and VPNs

Table 1: Comparison of Internet, Intranet, and Extranet

5 Maintaining Security in Intranets and Extranets

- Access Control
  - Ensures only authorized internal users can access certain resources
  - Role Based
- Encryption
  - Protects data being transmitted and sniffed across the network

- Firewalls and VPN
  - Protects against unauthorized access from the public internet

5.1 Firewalls

- Packet is forwarded $\iff$ it has an **allowed role**
  - If not, it is blocked
- This allows the whitelisting or blacklisting of certain *trusted* IP addresses
- Can block all incoming traffic on a specific port

6 VPNs

- Creates a secure connection between users and the internet
- Protects some data from external threats

6.1 How it works

- User connects to VPN service
- VPN client encrypts data before it leaves device
- Data sent through **secure tunnel** to the VPN server
- VPN server decrypts the data and forwards it to the destination
- Response from destination is then ecnrypted and sent back to the user through the same secure tunnel

6.2 Why use a VPN

- Security
  - Encrypts and protects sensitive data
- Privacy
  - Masks IP addresses
- Bypass Geo-Restrictions and Censorship
- Secure remote access
  - You can connect to company resources from remote locations securely

6.3 Limitations

- Encryption overhead slows down the spead of internet
- Cost of maintenance is high
- VPN does not ensure end-to-end encryption
  - VPN service could get a court order for example

6.4 Protocols

- PPTP
  - P2P Tunneling Protocol
  - Old, Fast, and not particularly secure
- L2TP/IPSec

  - Layer 2 Tunneling Protocol with IPsec
  - Commonly used and more secure
- IKEv2/IPSec
  - Internet Key Exchange Version 2
  - Very fast, secure, and ideal for mobile devices