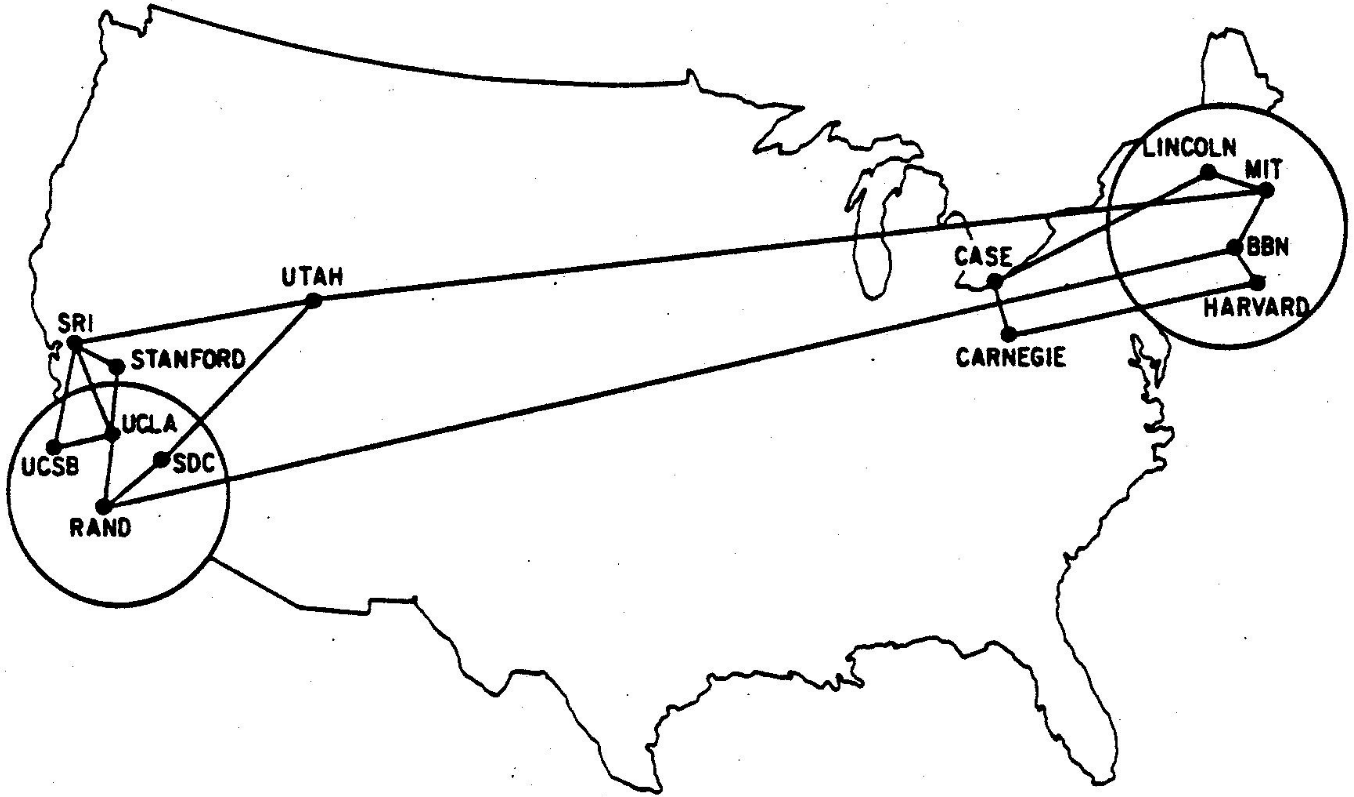
AN OVERVIEW OF FIREWALLS

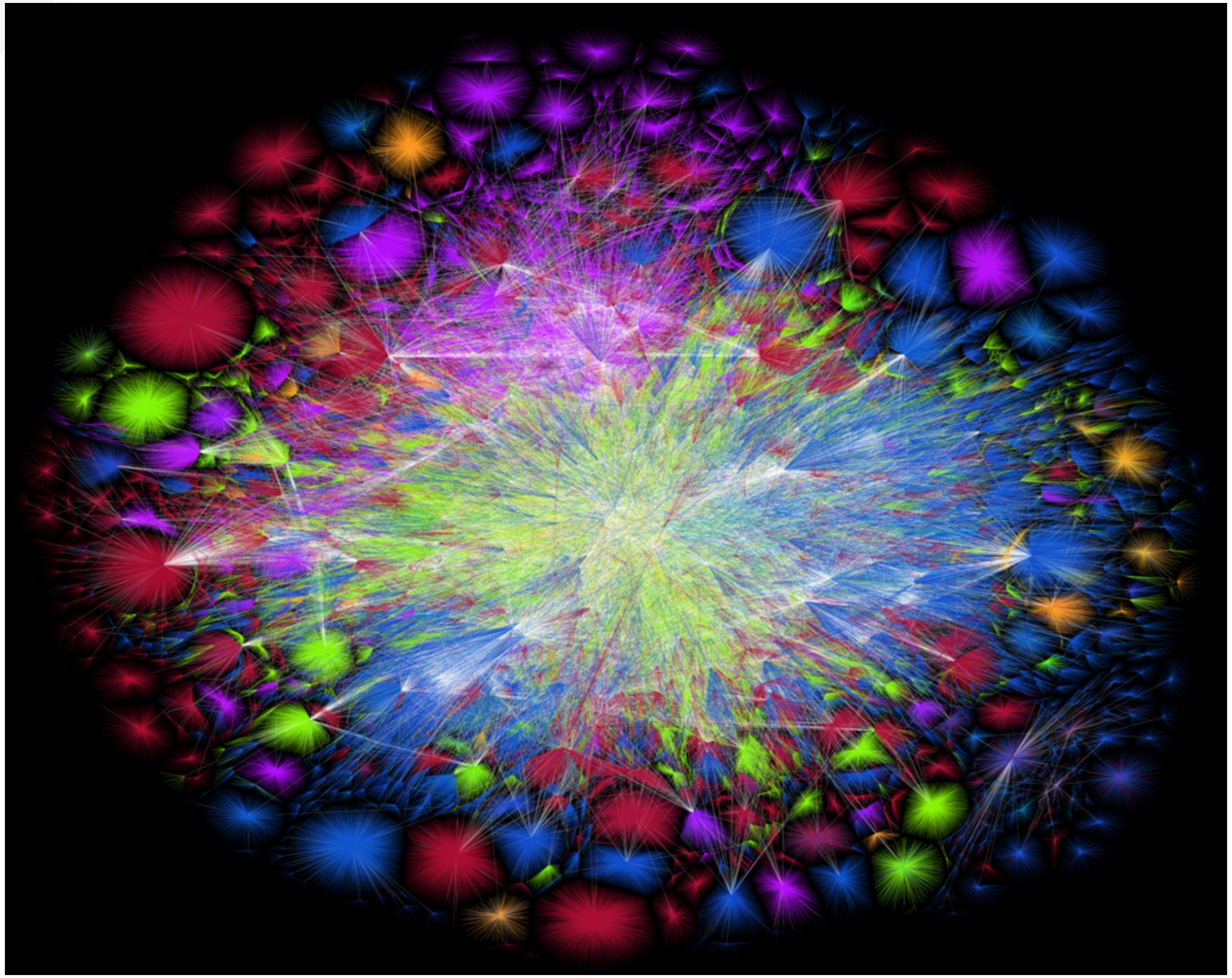
SASHANK NARAIN

THE INTERNET IN 1970



ARPANET (1970)

THE INTERNET NOW...

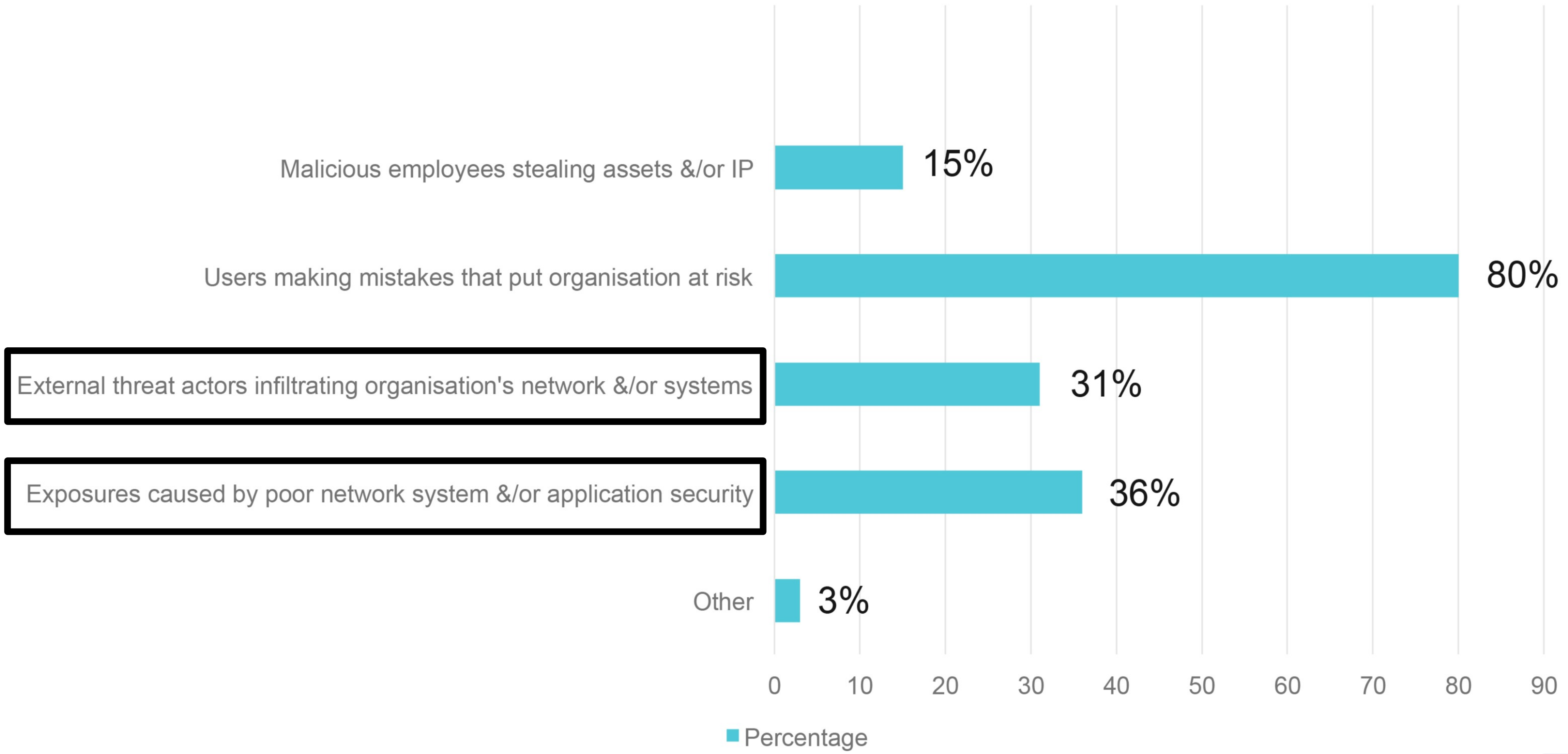


Map of the Internet in 2020

Source: Opte Project

NETWORKS ARE ALWAYS UNDER THREAT

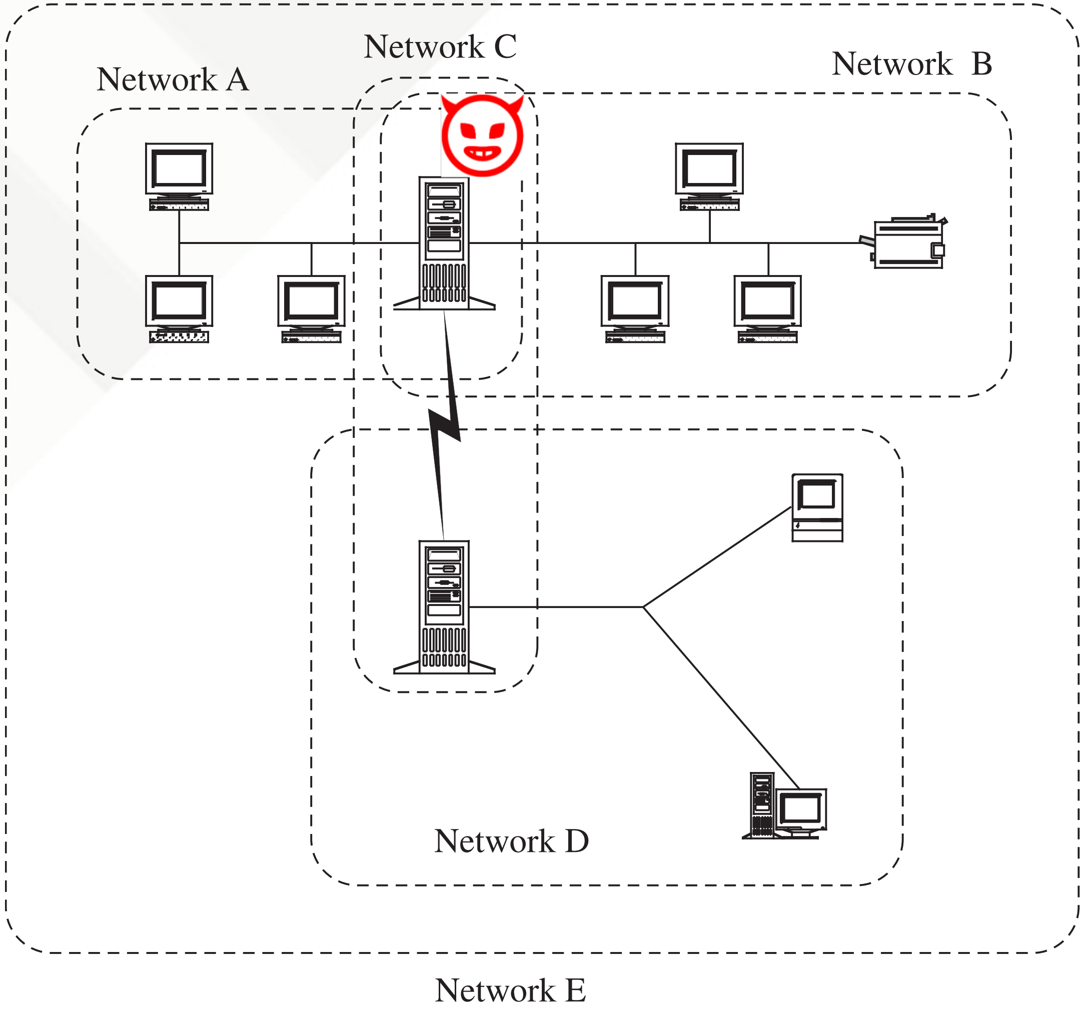
Cyber security threats leading to security incidents within the past 12 months



Source: SolarWinds

Learning with Purpose

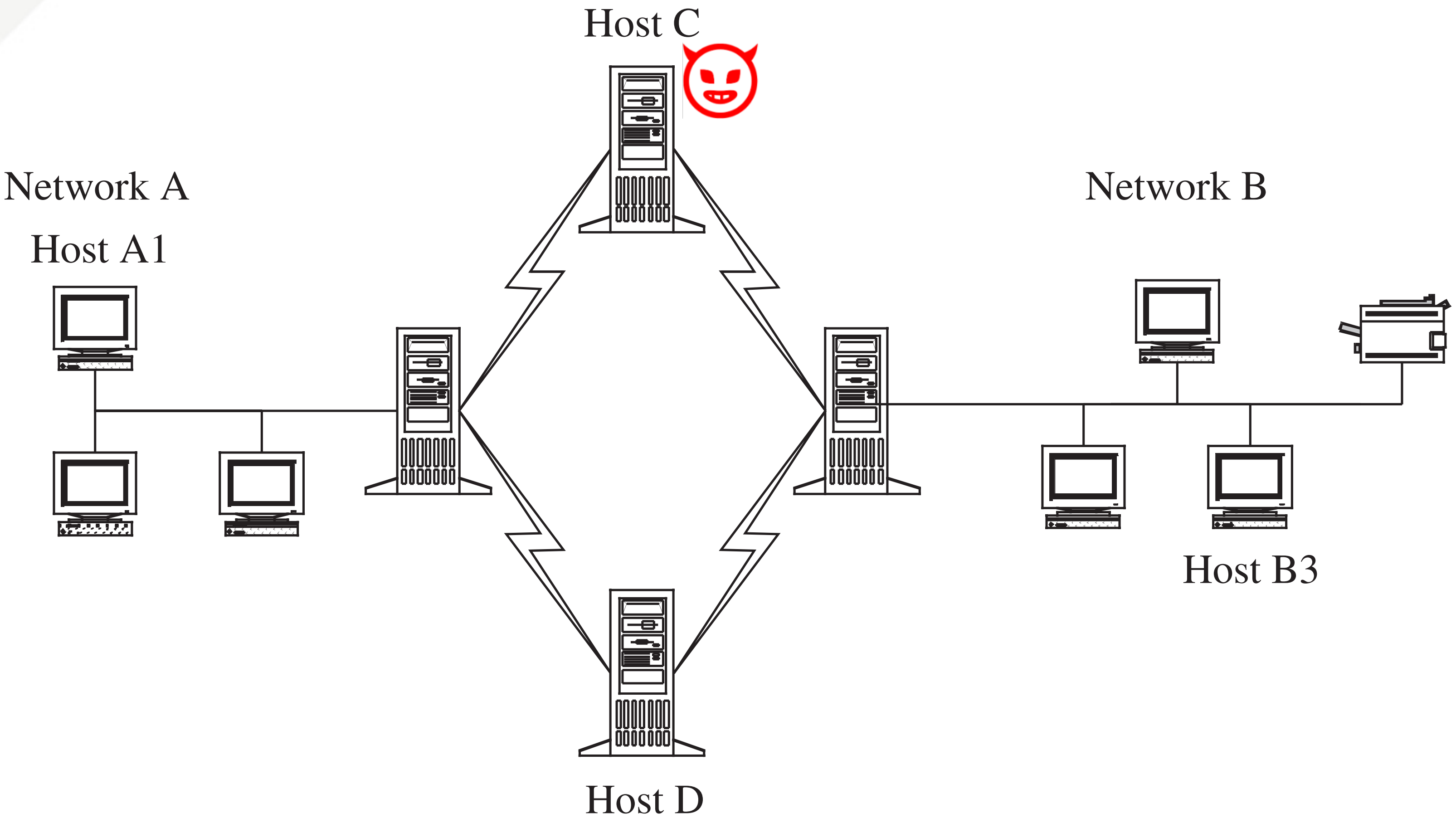
CAUSES OF NETWORK THREATS - UNKNOWN PERIMETER



- Networks change all the time
  - Large networks are **difficult to manage**
  - **Nodes may be in multiple networks**

CAUSES OF NETWORK THREATS - UNKNOWN PATH

- There may be **many paths**, including untrustworthy ones, from one node to another



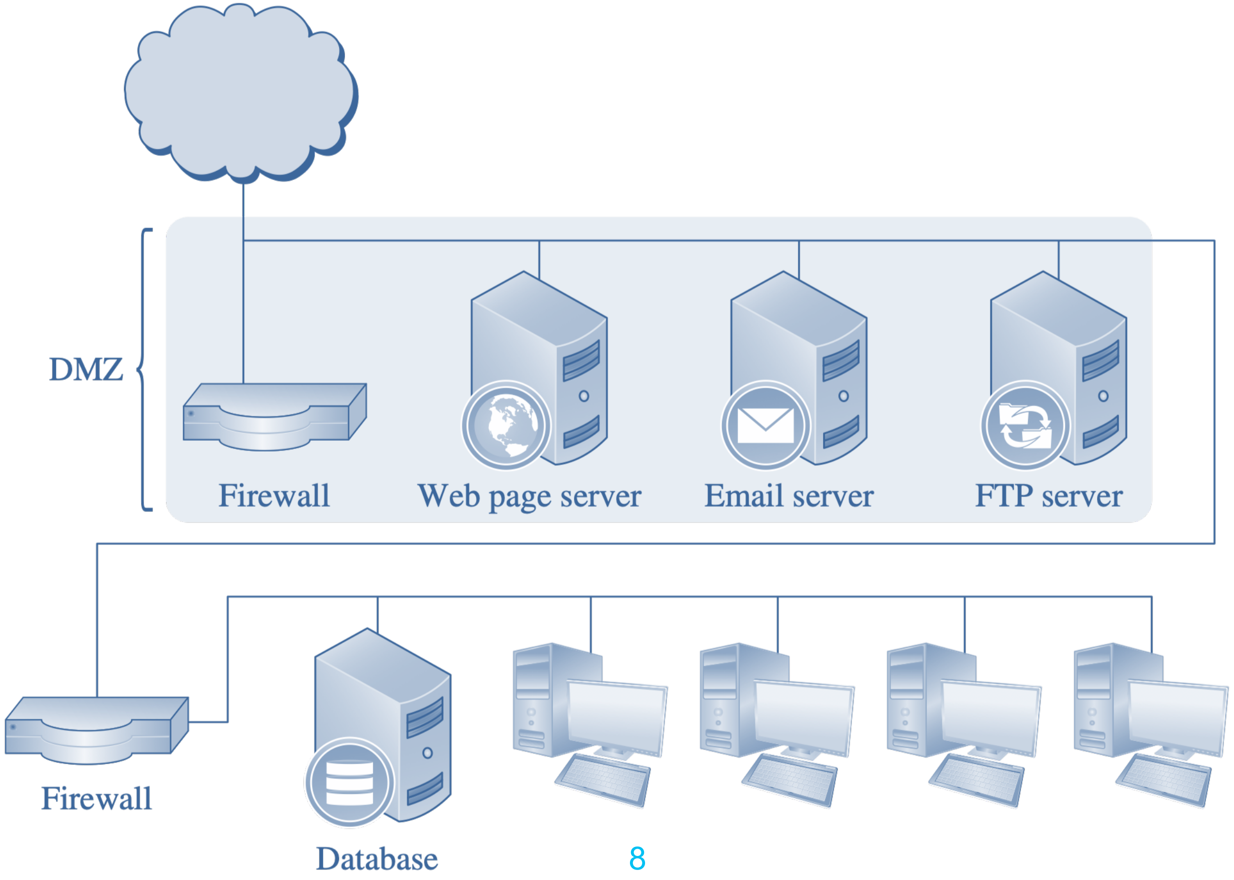
SCANNING A NETWORK FOR AVAILABLE SERVERS

- **nmap** – Very popular open-source **network scanner**
  - Scan wide-range of devices in the network

nmap Demo

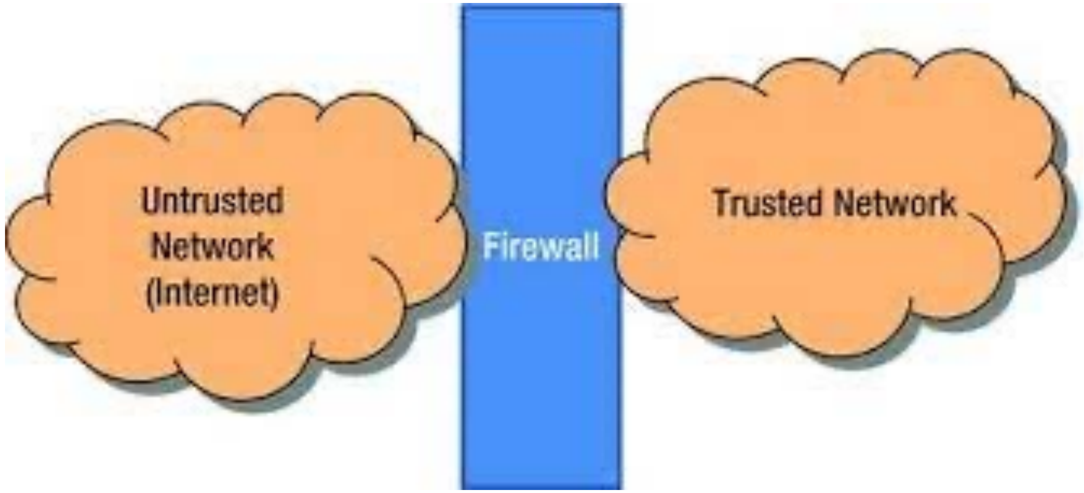
PROTECTION FROM NETWORK ATTACKS

- Put **nodes into zones** based on their sensitivity
- Implement a **firewall for each zone (Network Firewall)**
- Implement a **firewall on each node (Host-based Firewall)**



WHAT IS A FIREWALL?

- **Firewall - A device that filters data between a trusted or “inside” network and untrusted or “outside” network**
  - Defines a **set of rules that determine what can or cannot pass** through

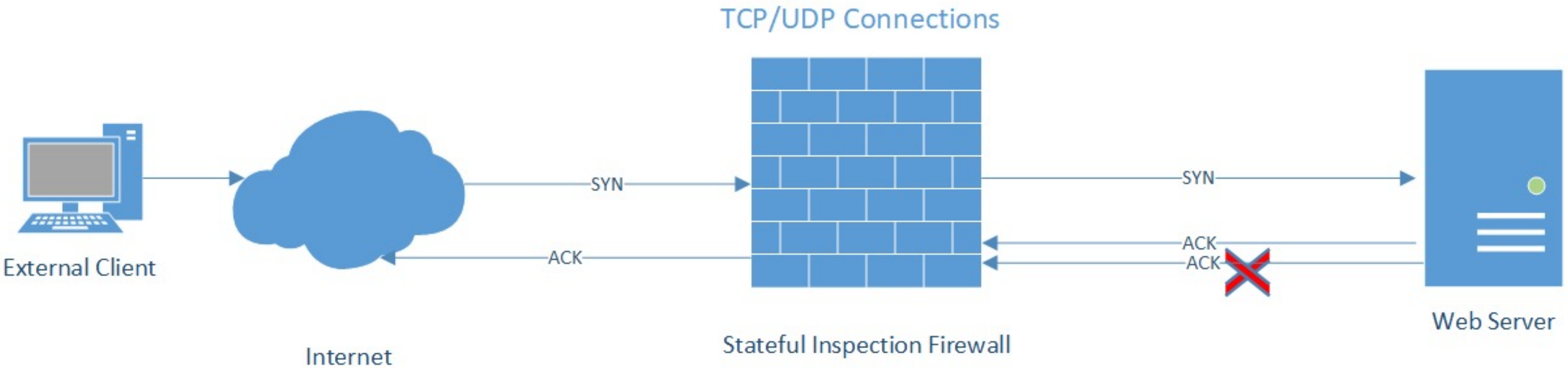


A REAL-WORLD ANALOGY OF FIREWALLS

Source: https://www.publicdomainpictures.net/en/view-image.php?image=7785

STATEFUL INSPECTION FIREWALL

- **Most common** type of firewall
- Firewall **decisions based on packet type and state information**
  - States: related, established



EXAMPLE OF A STATEFUL INSPECTION FIREWALL

- Assuming **X is the IP address** of a node

Rule No	Protocol	Source IP	Destination IP	Destination Port	Action
1	TCP	Any	X	22 (SSH)	Allow
2	UDP	X	Any	53 (DNS)	Allow
3	TCP	X	Any	80 (HTTP)	Allow
4	TCP	X	Any	443 (HTTPS)	Allow
5	Any	Any	Any	Any	Deny

LINUX UNCOMPLICATED FIREWALL (UFW) EXAMPLE

```
$ ufw default deny incoming
$ ufw default deny outgoing
$ ufw allow in 22/tcp
$ ufw allow out 53/udp
$ ufw allow out 80/tcp
$ ufw allow out 443/tcp
$ ufw enable
```

Rule No	Protocol	Source IP	Destination IP	Destination Port	Action
1	TCP	Any	X	22 (SSH)	Allow
2	UDP	X	Any	53 (DNS)	Allow
3	TCP	X	Any	80 (HTTP)	Allow
4	TCP	X	Any	443 (HTTPS)	Allow
5	Any	Any	Any	Any	Deny

LINUX UNCOMPLICATED FIREWALL (UFW) DEMO

UFW Demo