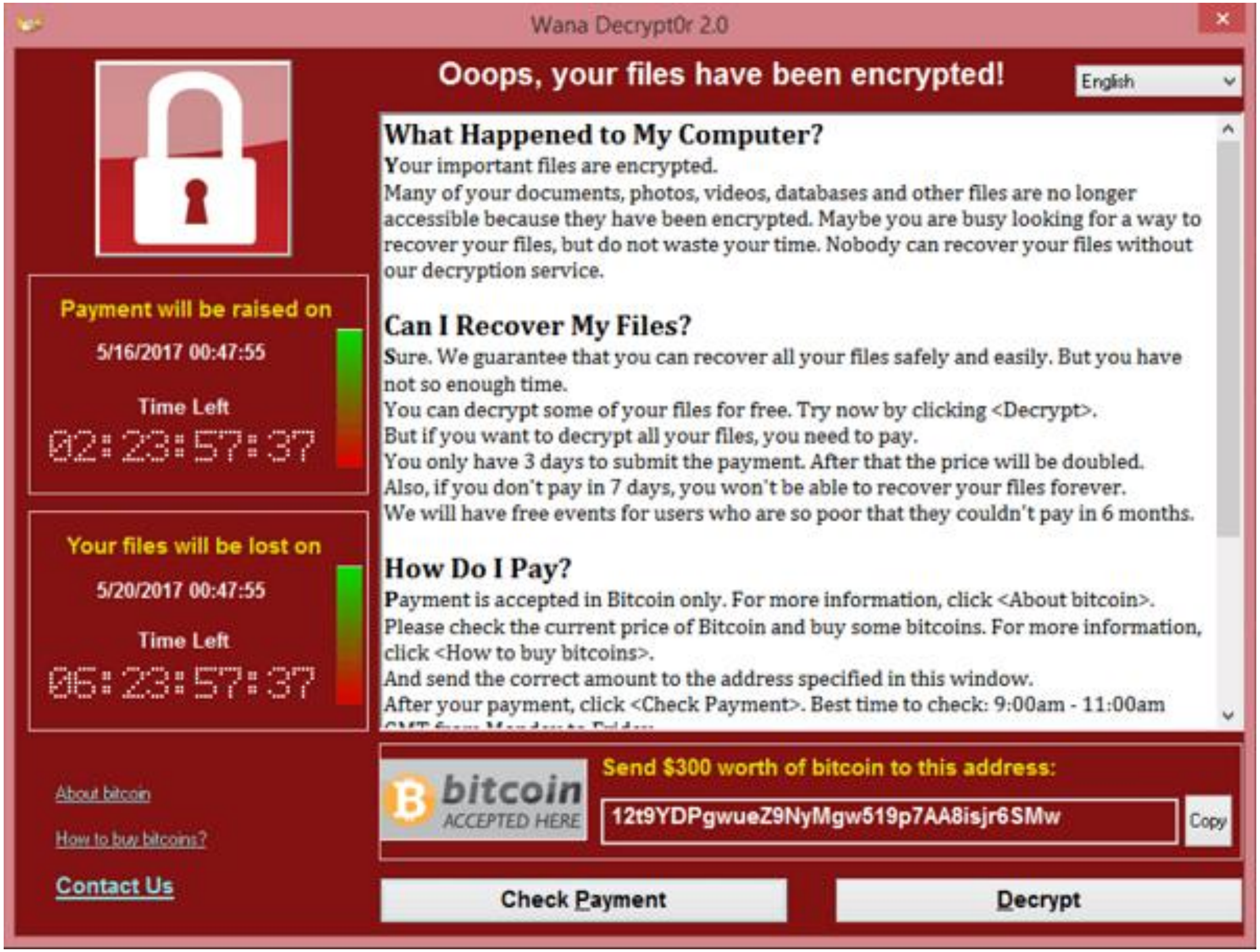
Firewalls and Network Security

Objectives

- The rise of cybercrimes
- Different Types of cyber attacks
- Types of network attacks
- Network security control
- Port scanning
- Segmenting networks
- What is a firewall
- How firewalls work
  - Packet filtering gateways
  - Stateful inspection firewalls
  - Application proxy gateways
  - Circuit-Level Gateways
  - Guard firewalls
  - Personal firewalls
- Network address translation
- Establishing a network security perimeter

The Rise of Cybercrimes

- WannaCry Ransomware attack



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

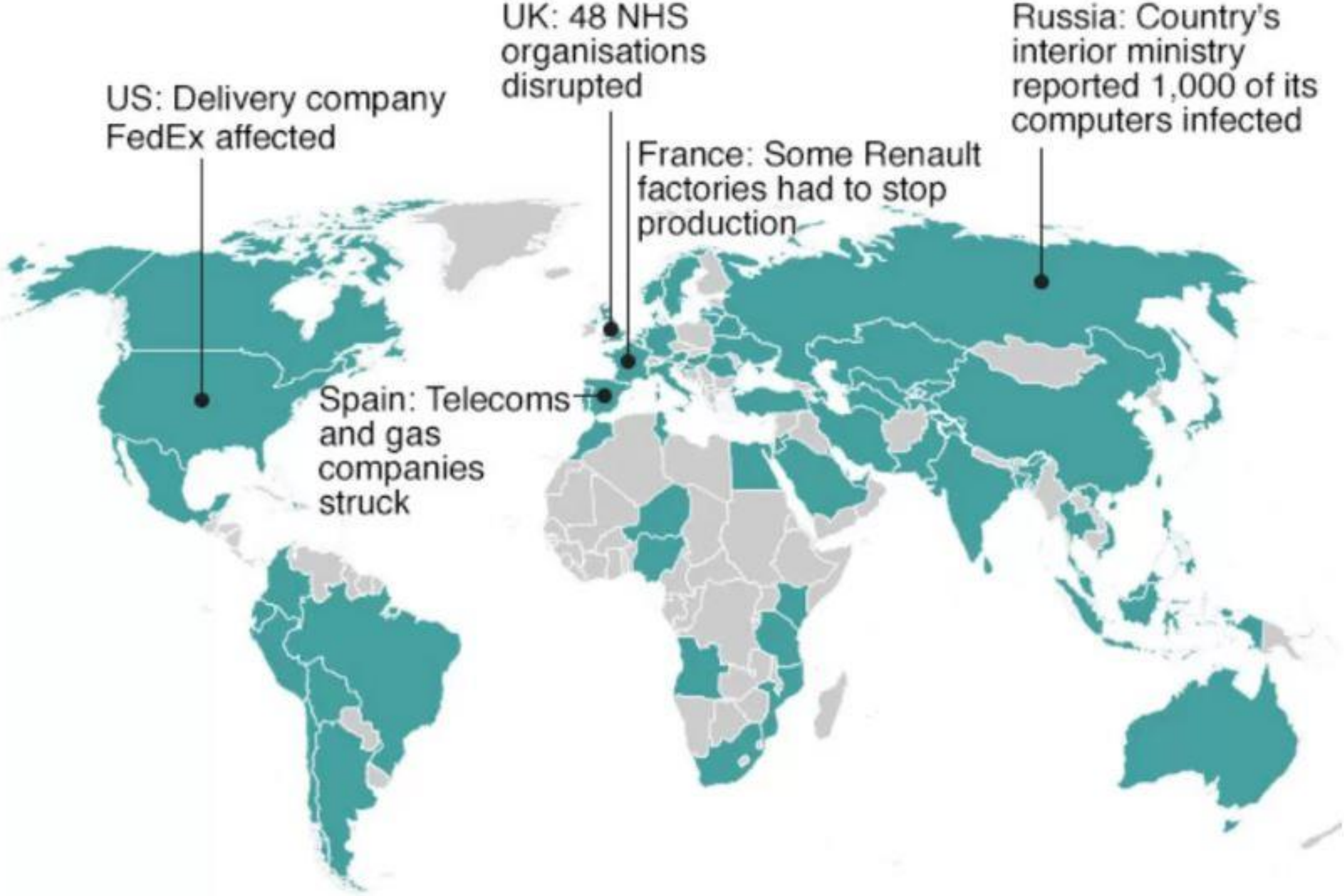
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

https://www.bbc.co.uk/news/world-europe-39907965



US: Delivery company FedEx affected

UK: 48 NHS organisations disrupted

France: Some Renault factories had to stop production

Russia: Country's interior ministry reported 1,000 of its computers infected

Spain: Telecoms and gas companies struck

*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Noway, where incidents have been reported since

Source: Kaspersky Lab's Global Research & Analysis Team

BBC

https://www.bbc.co.uk/news/world-europe-39907965

The Rise of Cybercrimes

- Dunkin' Donuts, February 2019
  - ➢ Dunkin' Falls Victim To Credential Stuffing Attack
  - ➢ The users' first and last names, and email addresses were stolen

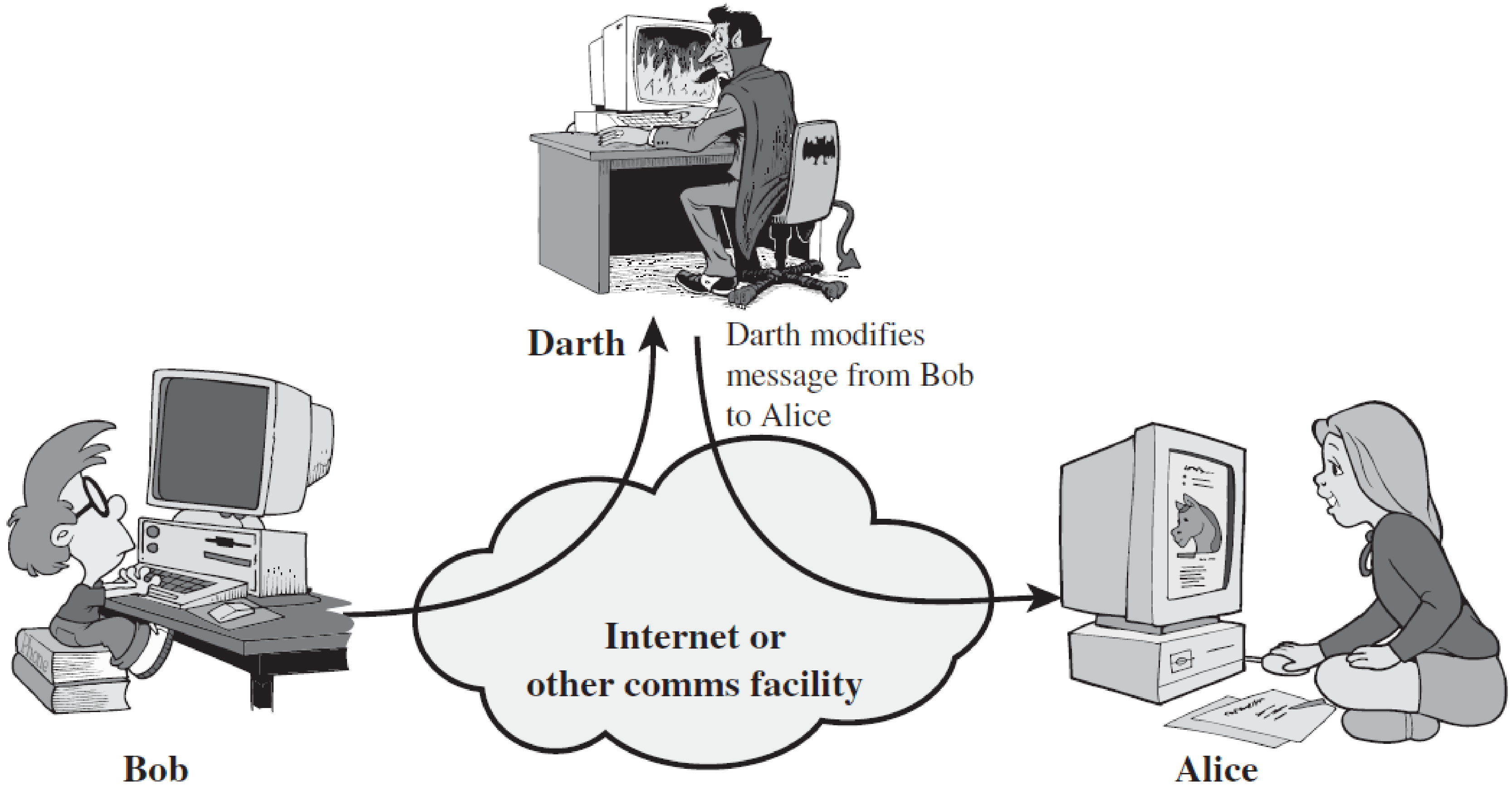
https://www.pymnts.com/news/retail/2023/will-consumers-pay-50-for-drugstore-brand-sunscreen/

Different Types of Cyber Attacks

- Malware Attack
- Social Engineering Attack
- Man in the Middle Attack
- Denial of Service Attack
- SQL Injection Attack
- Password Attack
- Advanced Persistent Threat

Types of Network Attacks

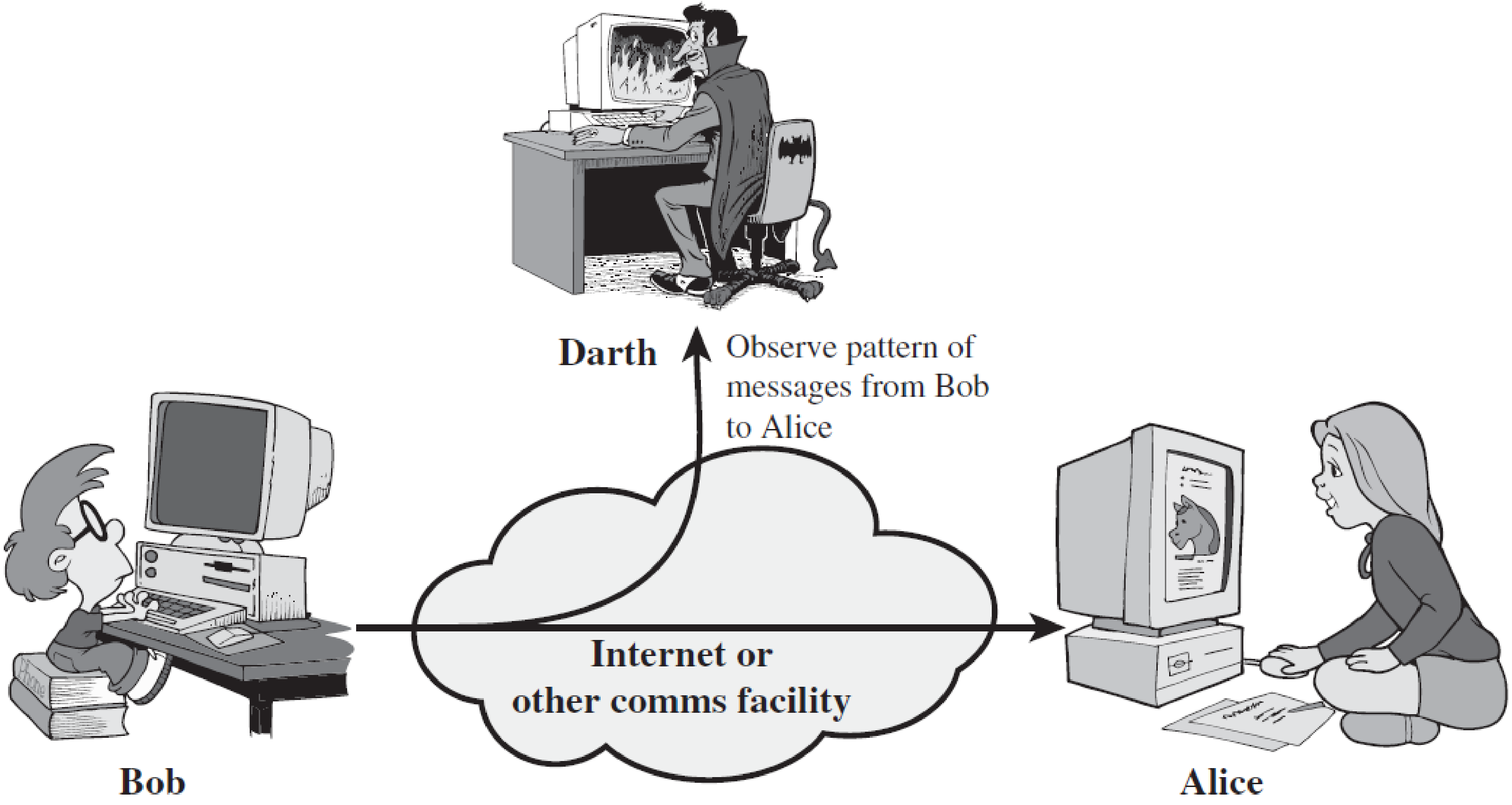
- Active Attack


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Source: Stallings, William. Network security essentials: Applications and standards, 4/e. Pearson Education, 2011.

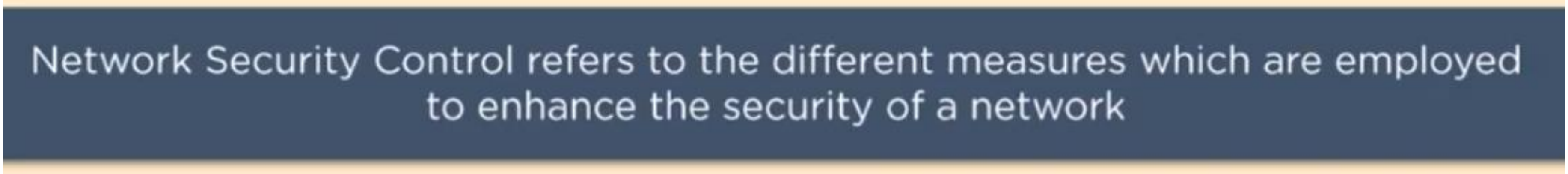
Types of Network Attacks

- Passive Attack


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

Source: Stallings, William. Network security essentials: Applications and standards, 4/e. Pearson Education, 2011.

Network Security Control

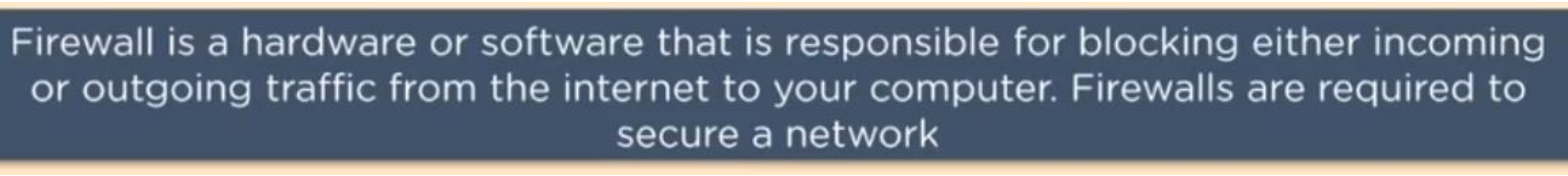


Network Security Control refers to the different measures which are employed to enhance the security of a network

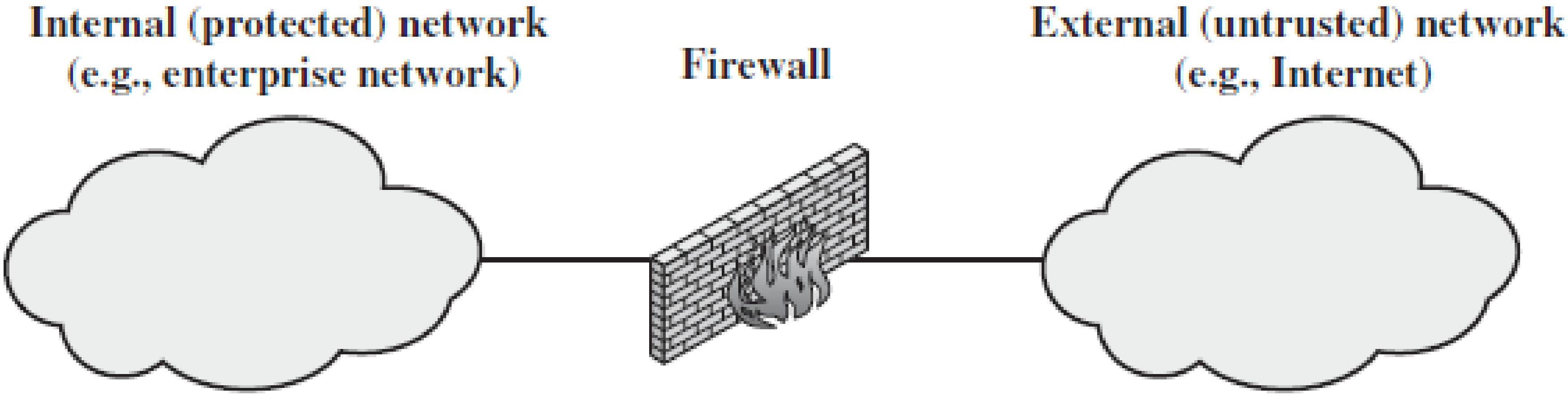
- Firewalls
- Intrusion Detection Systems (IDSs)
- Honeypots

Network Security Control

- Firewall



Firewall is a hardware or software that is responsible for blocking either incoming or outgoing traffic from the internet to your computer. Firewalls are required to secure a network

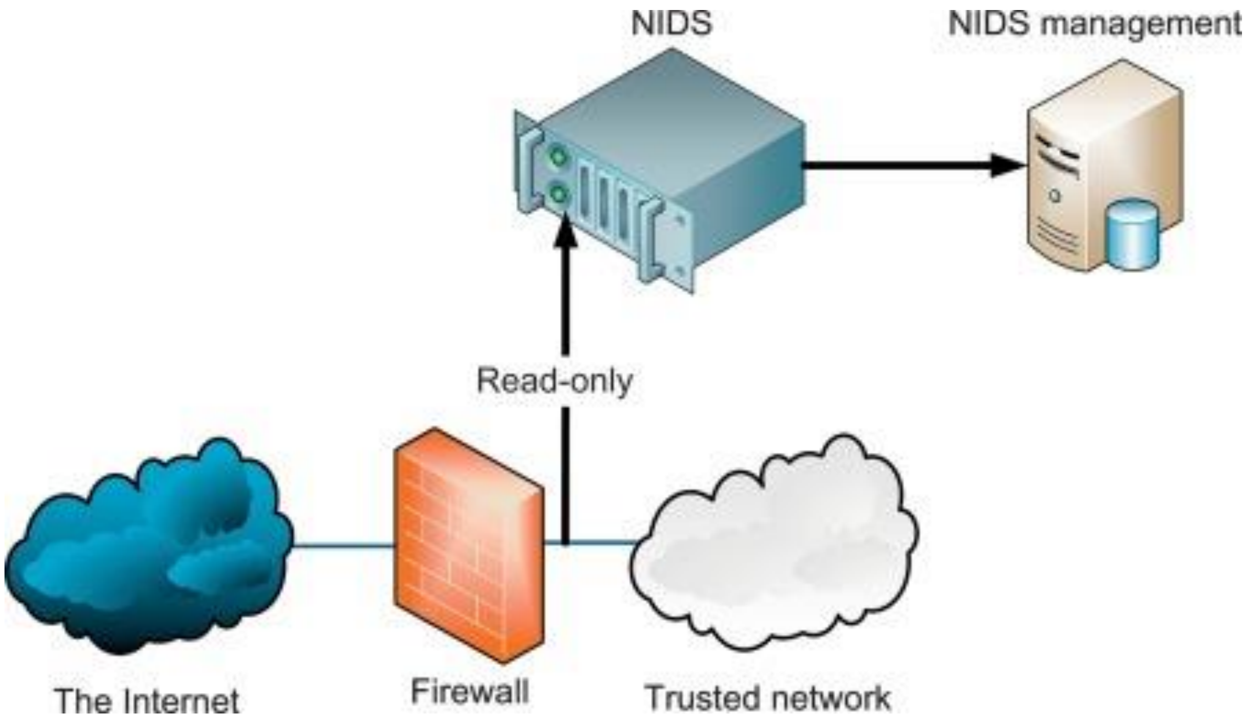

Internal (protected) network
(e.g., enterprise network)
Firewall
External (untrusted) network
(e.g., Internet)

Source: Stallings, William. Network security essentials: Applications and standards, 4/e. Pearson Education, 2011.

Network Security Control

- Intrusion Detection System (IDS)

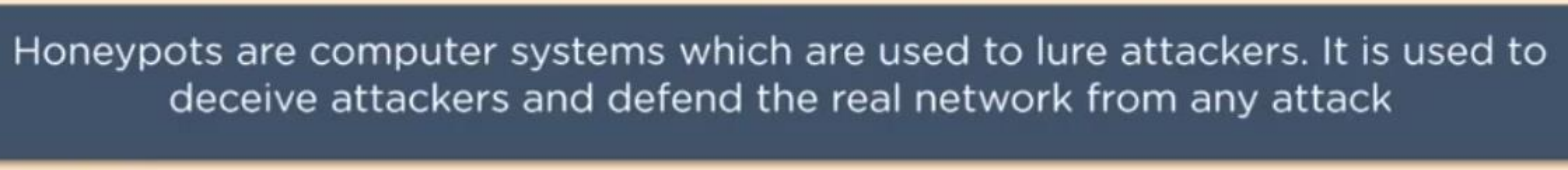
Intrusion Detection System (IDS) is designed to detect unauthorized access to a system. It is used together with a firewall and a router



Source: Eric Conrad, Seth Misenar, Joshua Feldman. Eleventh Hour CISSP®: Study Guide. Syngress, Elsevier Inc. 2017.

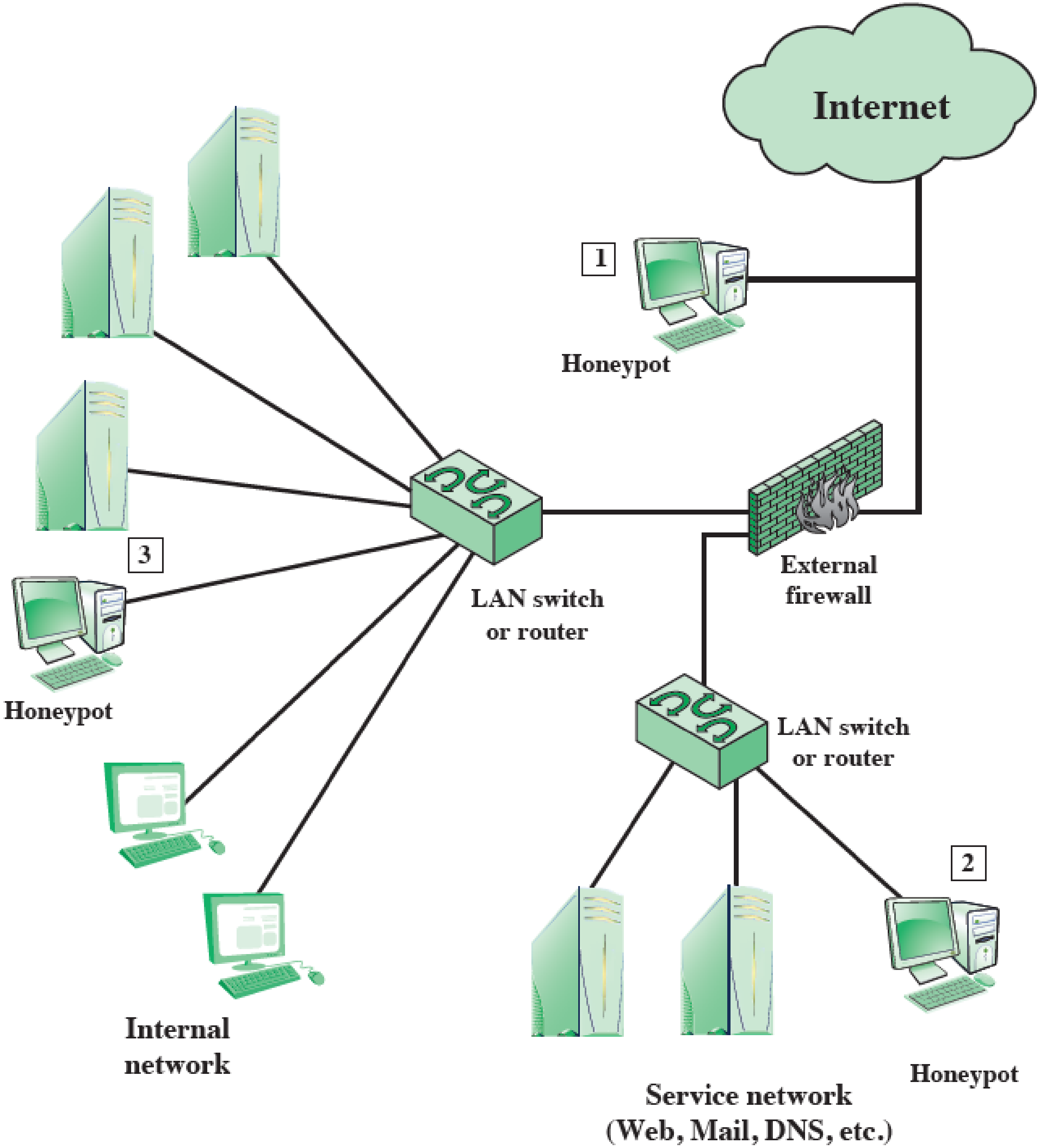
Network Security Control

- Honeypots



Honeypots are computer systems which are used to lure attackers. It is used to deceive attackers and defend the real network from any attack

Example of Honeypot Deployment



Source: Stallings, William. Network security essentials: Applications and standards, 6/e. Pearson Education, 2017.

Computer Networks

- A computer network is a set of communication channels that interconnects computer devices and enables them to exchange data electronically

- Basic terminology
  - Node
  - Host
  - Link

Network Advantages and Vulnerabilities

- Network advantages
  - Resource sharing
  - Distribution of workload
  - Increased reliability
  - Expandability and scalability

- Several characteristics make networks vulnerable to attack
  - Anonymity
  - Many points of attack
  - Resource and workload sharing
  - System complexity
  - Unknown boundary

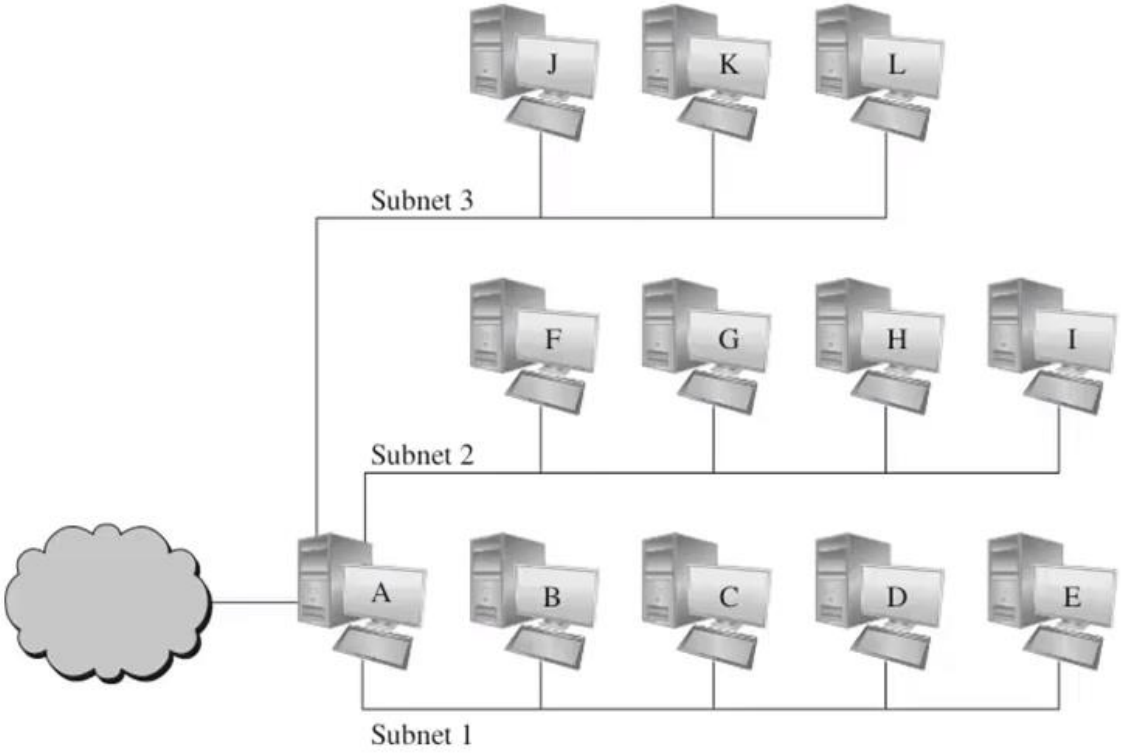
Port Scanning

- A port scanner is a software that is design to examine one or more IP addresses and record which ports are open and which known vulnerabilities are present
    - Open, Accepted
    - Closed, Not Listening
    - Filtered, Dropped, Blocked

- A network administrator or security analyst can use a port scanner to evaluate the strength and weaknesses of a network

Segmenting Networks

- One way of controlling threats from port scanners is to implement a segmented network architecture



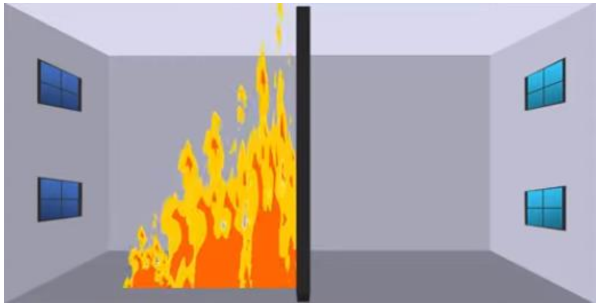
Firewalls

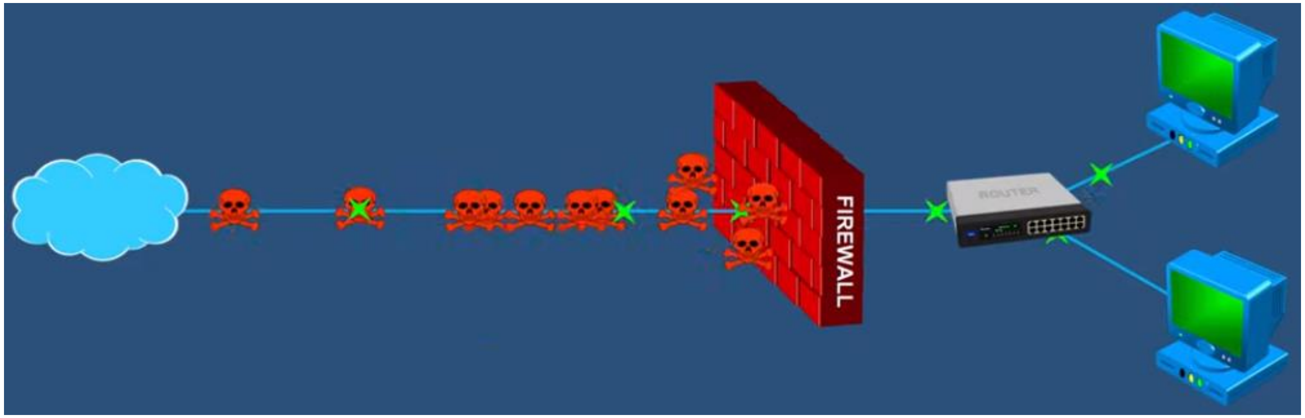
- A firewall is a device (hardware, software or both) that is designed to:
  - Prevent unauthorised outside users from accessing a network or workstation
  - Prevent inside users from transmitting sensitive information or accessing unsecured resources

- Properly implemented firewalls can reduce or eliminate many network threats

Firewalls

- A firewall creates a safety barrier between a private network and the public Internet





Firewall Security Policies

- A firewall security policy is a set of rules that a firewall relies upon to determine which traffic should be allowed to pass through a network boundary

- Examples of firewall security policy rules

- Firewalls may have a default security policy:
  - Default permit
  - Default deny

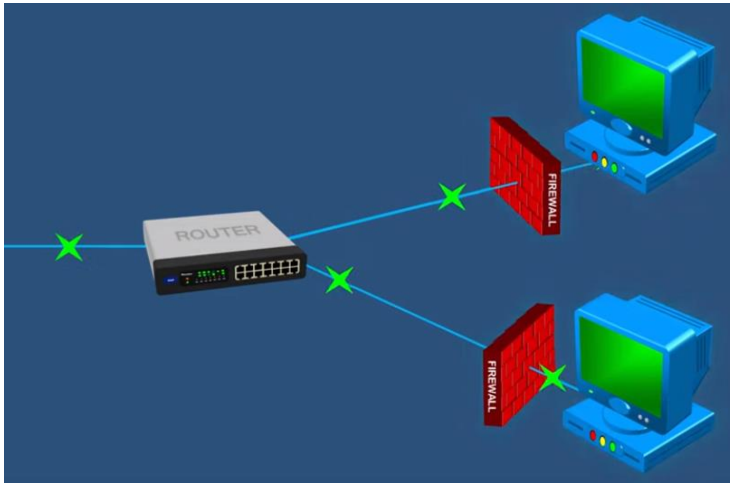
Firewall Rules

- Firewall rules can be based on:
  - IP addresses
  - Domain names
  - Protocols
  - Programs
  - Ports
  - Key words

- Access control list

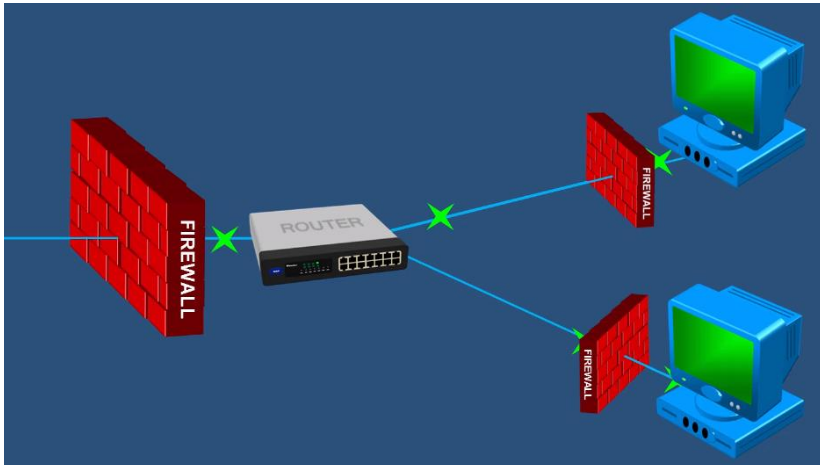
Firewall Types

- Host-based firewall
  - Software firewall that is installed on a computer
  - Protect that computer only
    - Microsoft windows firewall
    - 3rd party host-based firewall, e.g. Zone Alarm
    - A lot of antivirus programs come with a host-based firewall



Firewall Types

- Network-based firewall
  - Combination of hardware and software
  - Placed between a private network and the public Internet
  - Protect an entire network
    - ➢ Stand-alone firewall, large organisations
    - ➢ Built-in component of a router, smaller organisations
    - ➢ Deployed in a service provider's cloud infrastructure



OSI Model

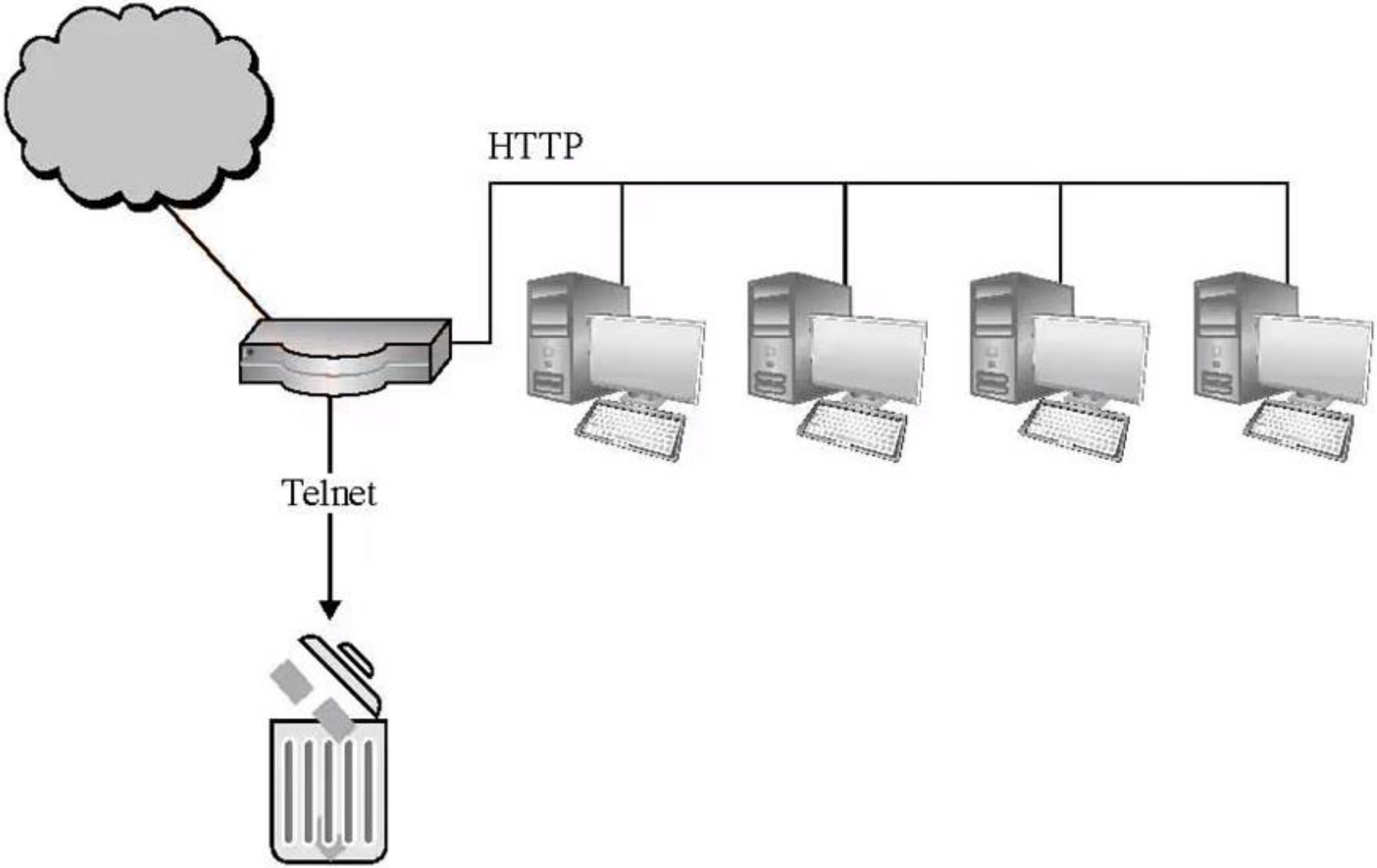
- The Open Systems Interconnection model is a conceptual model provides a standard for different computer systems to be able to communicate with each other
- OSI is not used, TCP/IP same concepts but a bit different layers
- Application (7)
- Presentation (6)
- Session (5)
- Transport (4)
- Network (3)
- Data link (2)
- Physical (1):
- To easy remember: **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing

Packet Filtering Gateways

- A packet filtering gateway (or screening router) is a type of firewall that regulates network boundary access by:
  - Examining the source and/or destination IP addresses for each packet
  - Examining the type of transport protocol for each packet (e.g. HTTP, FTP, telnet, etc.)
    - Port filtering

- Packets that are not acceptable in light of the firewalls security policy are discarded

Packet Filtering Gateways

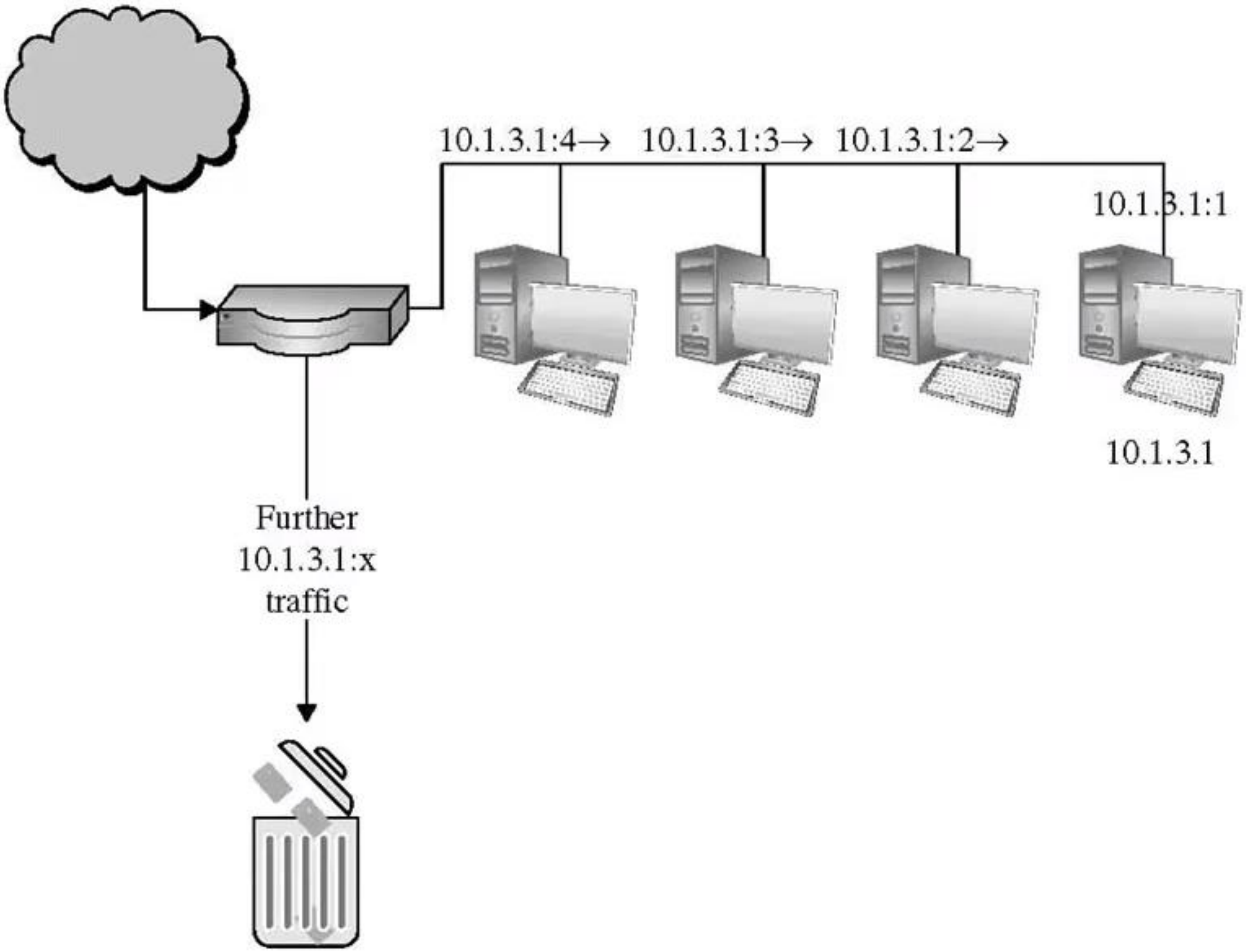


Stateful Inspection Firewalls

- Unlike a packet filtering gateway, a stateful inspection firewall considers the state or context of the packets that it evaluates

- The goal of a stateful inspection firewall is to identify hosts that represent a threat by accumulating evidence against them

Stateful Inspection Firewalls



Application Proxy Gateways

- An application proxy gateway (or bastion host) is a type of firewall that runs pseudo-applications which mimic the proper behavior of real applications

- The application proxy gateway can filter out unacceptable protocol commands while they are in transit between an application and a user

facebook

Email

Password

Log In

□ Keep me logged in

Forgot your password?

Facebook helps you connect and share with the people in your life.

Sign Up

It's free and always will be.

First Name:

Last Name:

Your Email:

Re-enter Email:

New Password:

I am: Select Sex:

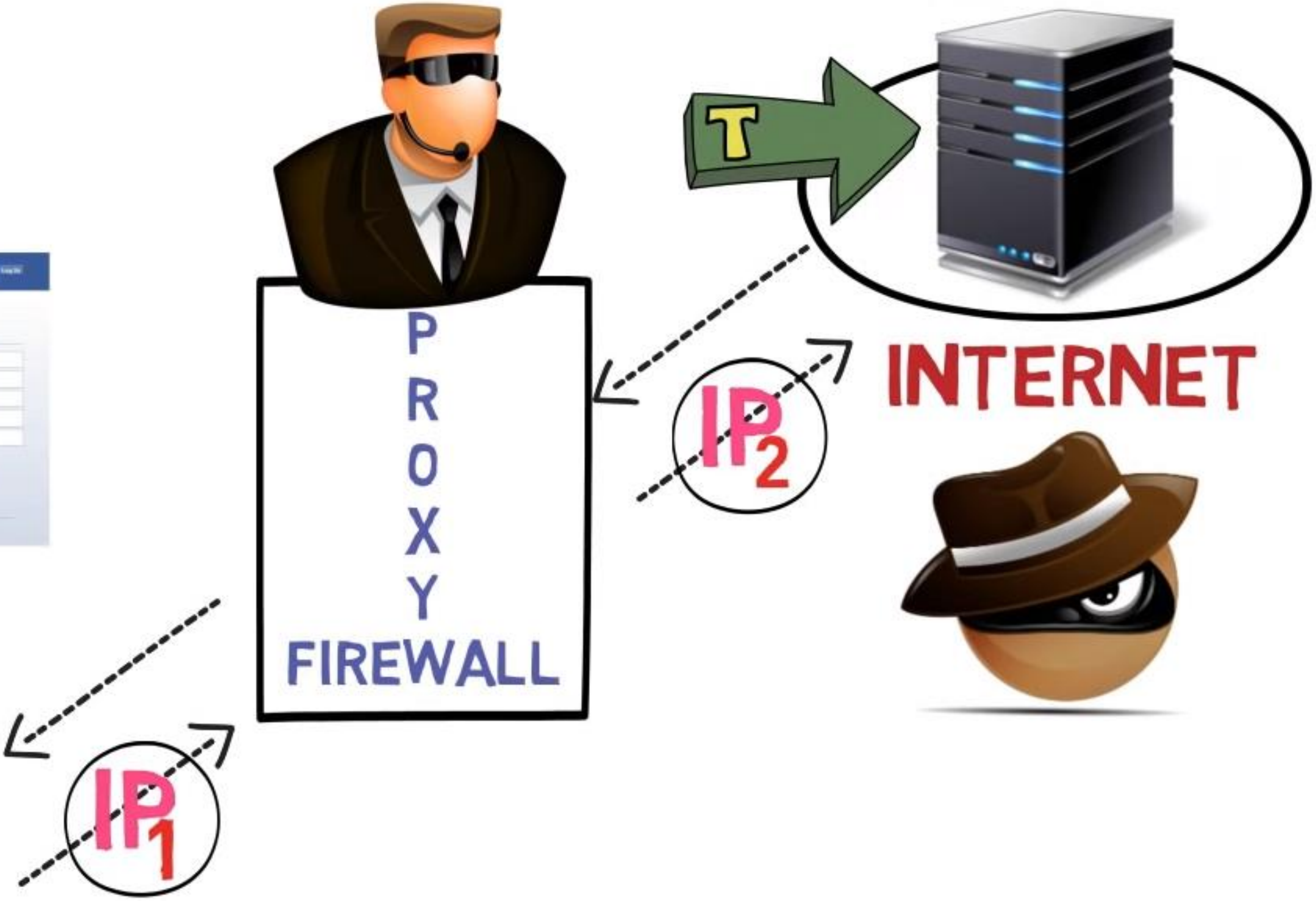
Birthday: Month: Day: Year:

Why do I need to provide my birthday?

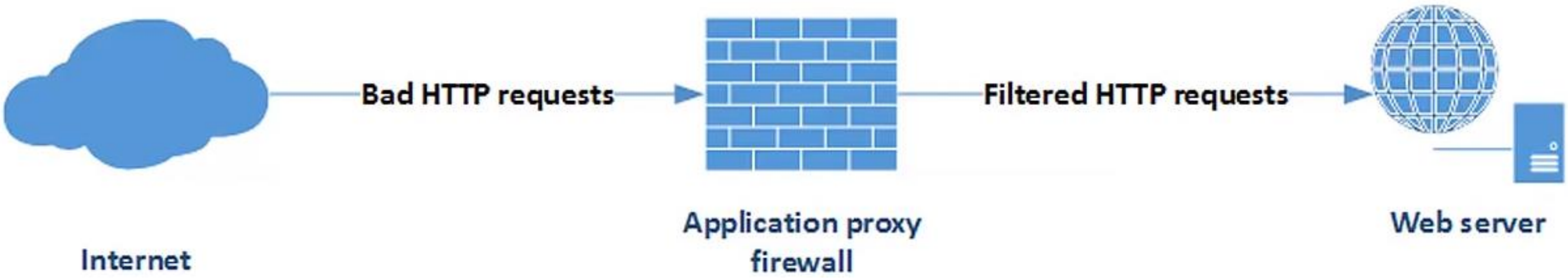
Sign Up

Create a Page for a celebrity, band or business.

WWW.FACEBOOK.COM



Application Proxy Gateways

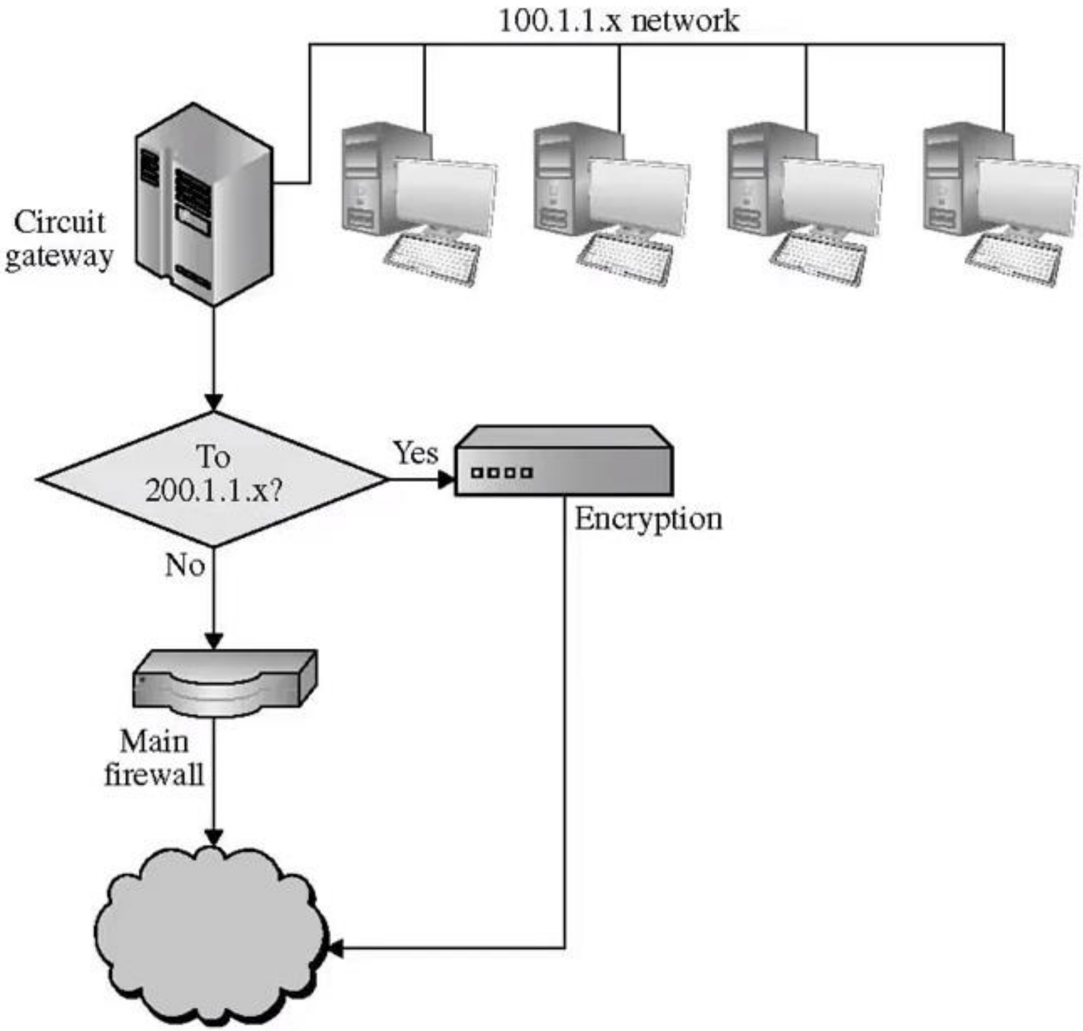


Circuit-Level Gateway

- A circuit-level gateway is a type of firewall that enables one network to become a virtual extension of another network

- Incoming / outgoing packets are examined to determine whether they are being sent to / received from the target network (examine the source and destination IP addresses)

Circuit-Level Gateway



Virtual Private Network

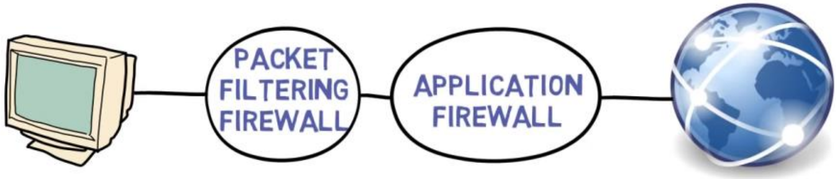
- VPN ensures your location stay private
- Your data is encrypted
- You can surf the web anonymously

Next-Generation Firewall (NGFW)

- NGFW offers the highest firewall protection
- Combines traditional firewall functions with advanced security features
  - deep packet inspection
  - intrusion prevention systems
  - application awareness
  - SSL/TLS decryption
  - threat intelligence

Which Firewall to Use

- Packet filtering gateway
  - Examines the packet header
  - Present in Internet routers
  - Doesn’t examine the packet payload
- Application proxy gateway
  - Runs pseudo-applications
  - Hides host’s' identities
  - Protects hosts from improperly formatted requests
  - Examines the packet payload
- Hybrid firewall



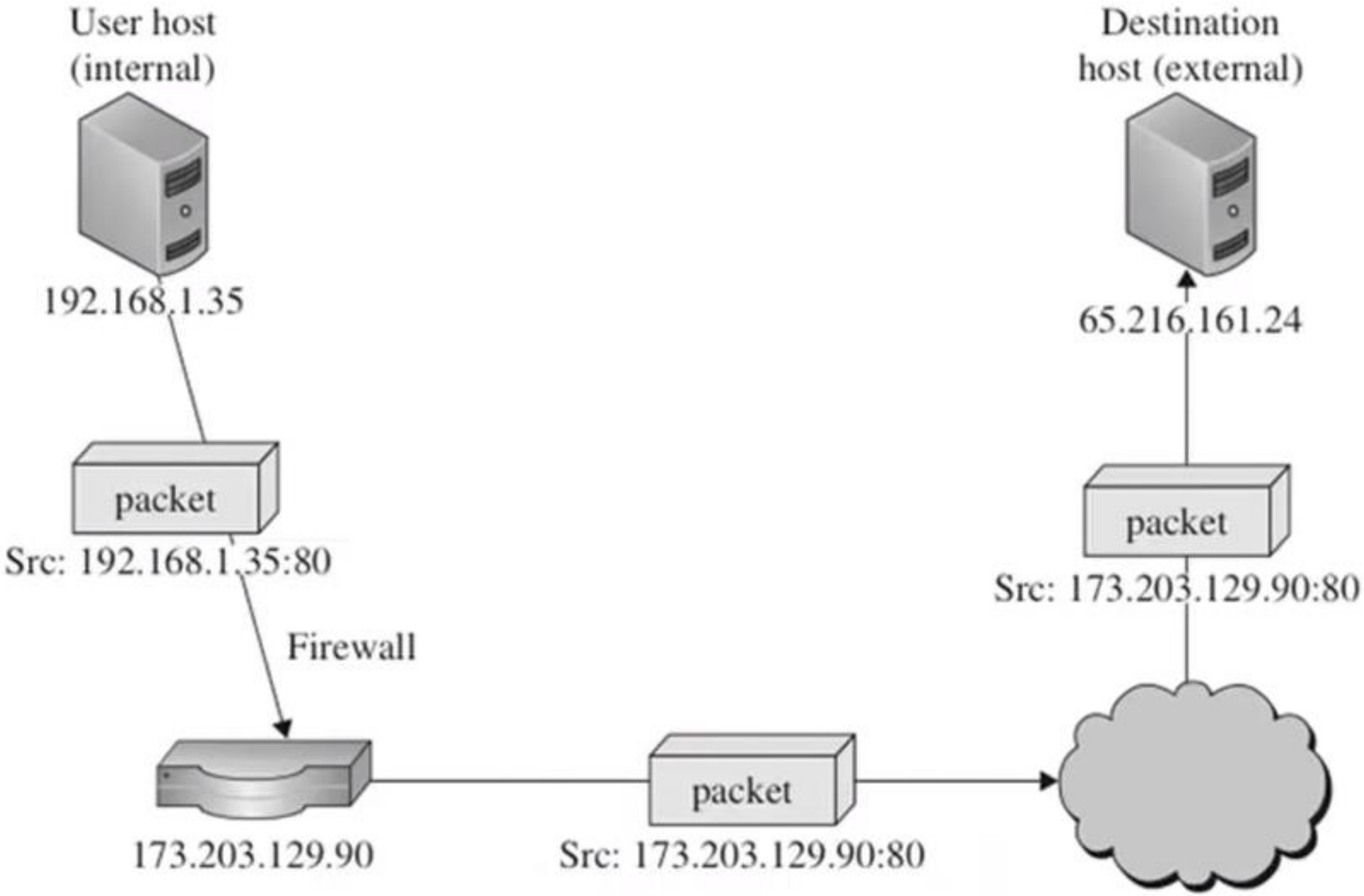
- Circuit-level gateway
  - Implements a virtual private network
- Next-Generation Firewall
  - Combines traditional firewall functions with advanced threat protection features
- Personal firewall
  - Protects only one host

Network Address Translation

- Hosts inside of a network boundary often expose their IP addresses to the outside world in order to enable communication

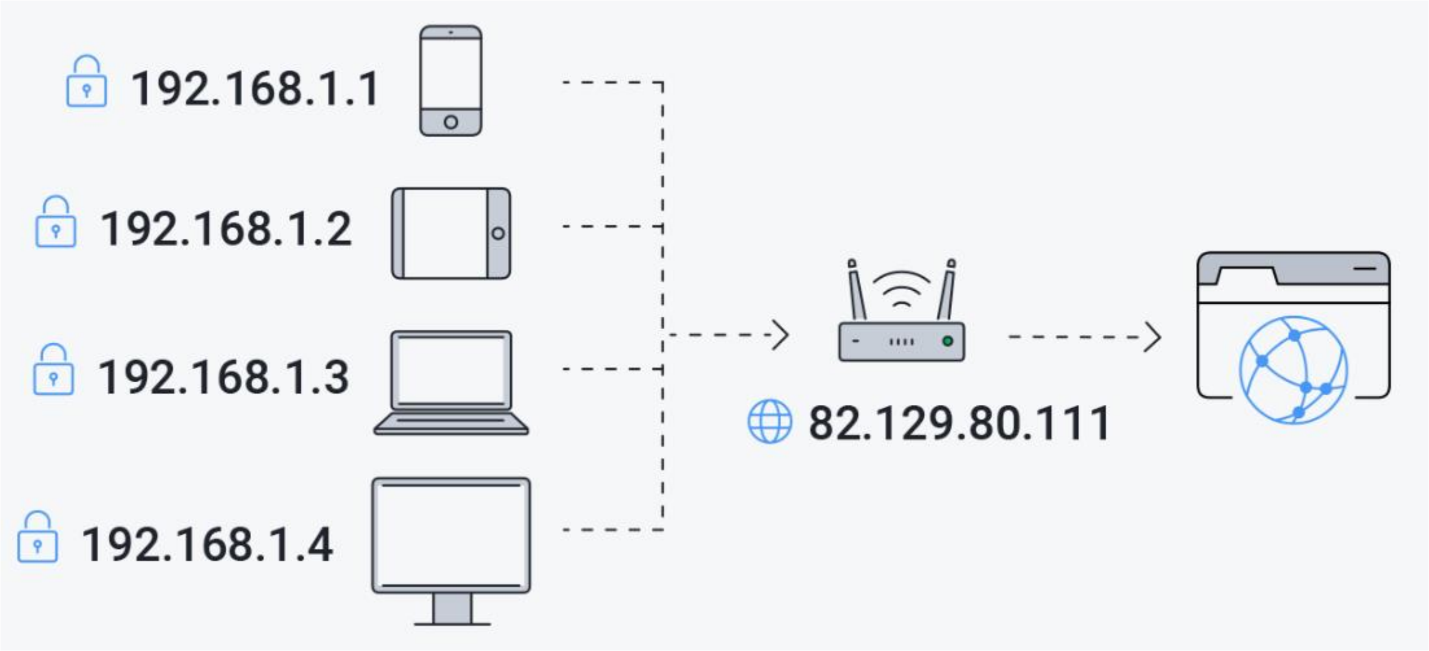
- A firewall can implement Network Address Translation (NAT) in order to hide the structure of an internal network from the outside world

Network Address Translation



Network Address Translation

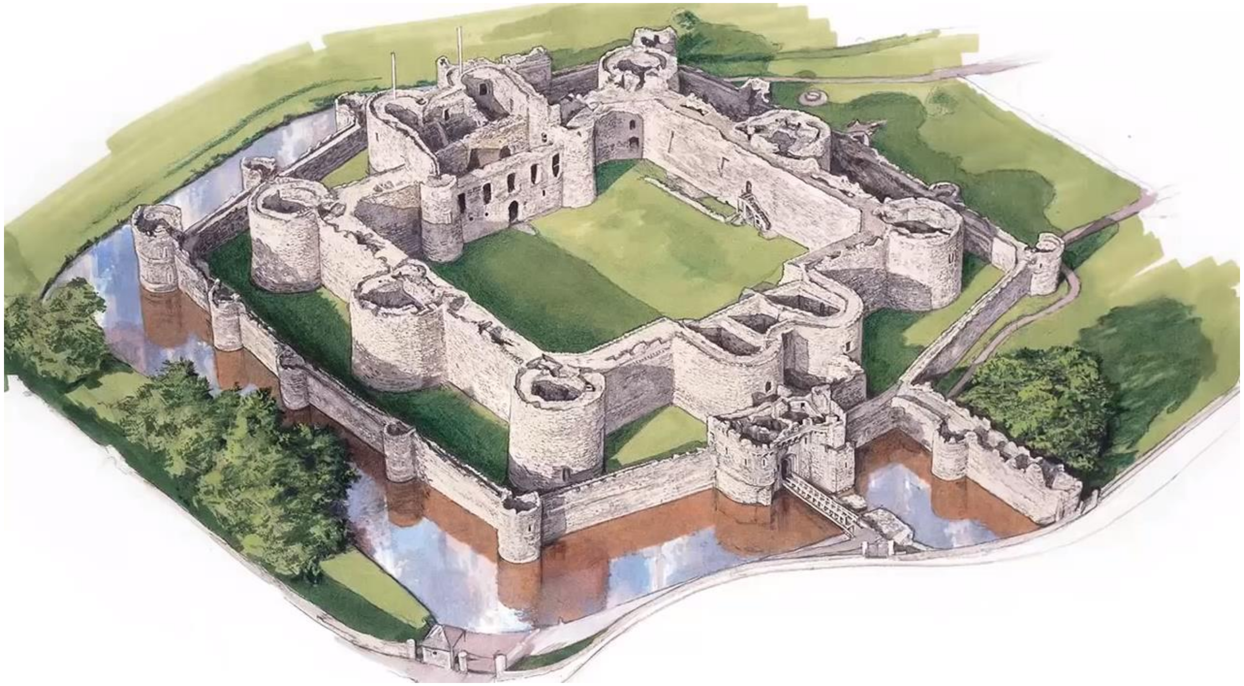
- NAT helps preserve the limited amount of IPv4 Public IP addresses
  - Public IP addresses
  - Private IP addresses
- IPv6, new generation of IP addresses



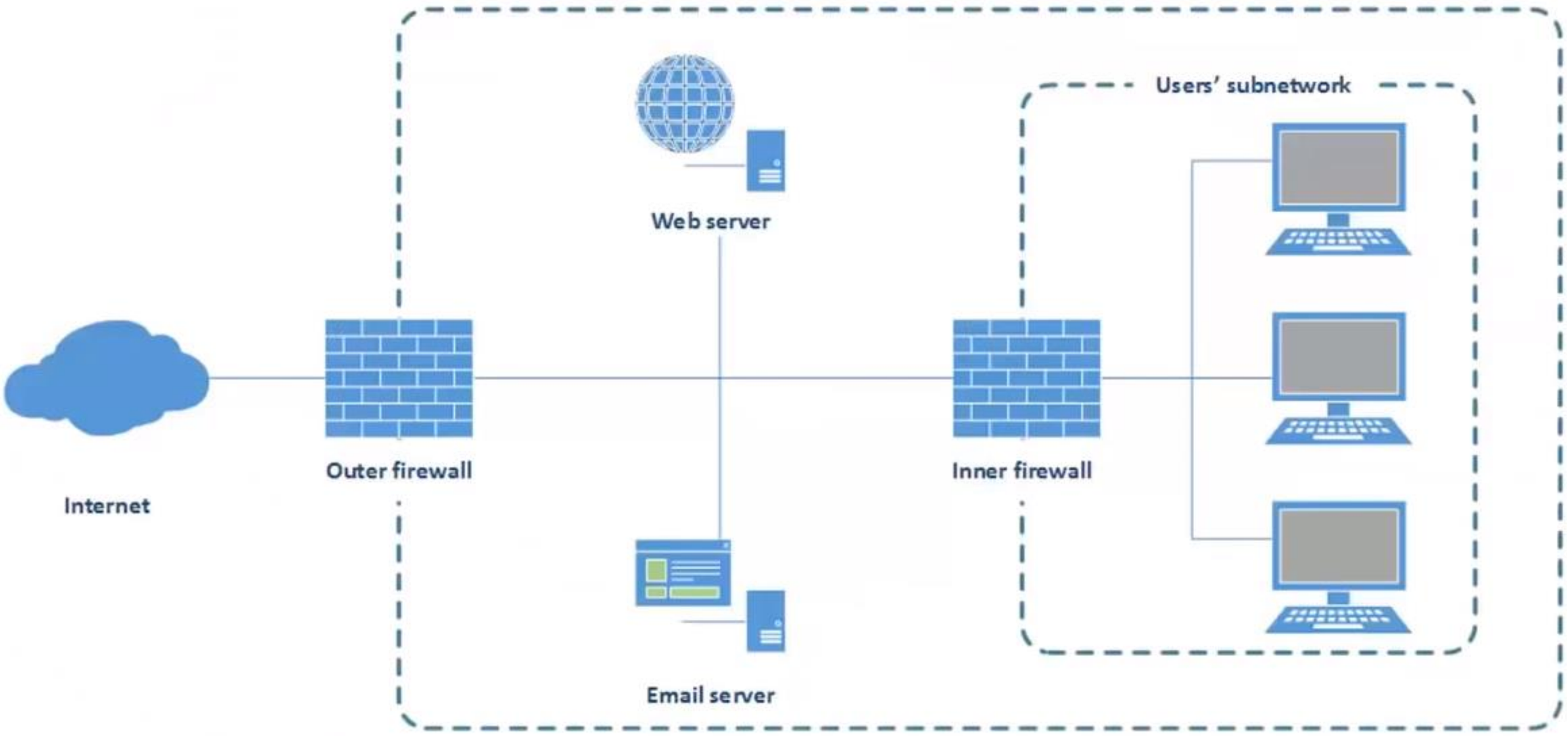
Source: https://www.avg.com/en/signal/public-vs-private-ip-address

Establishing a Network Security Perimeter

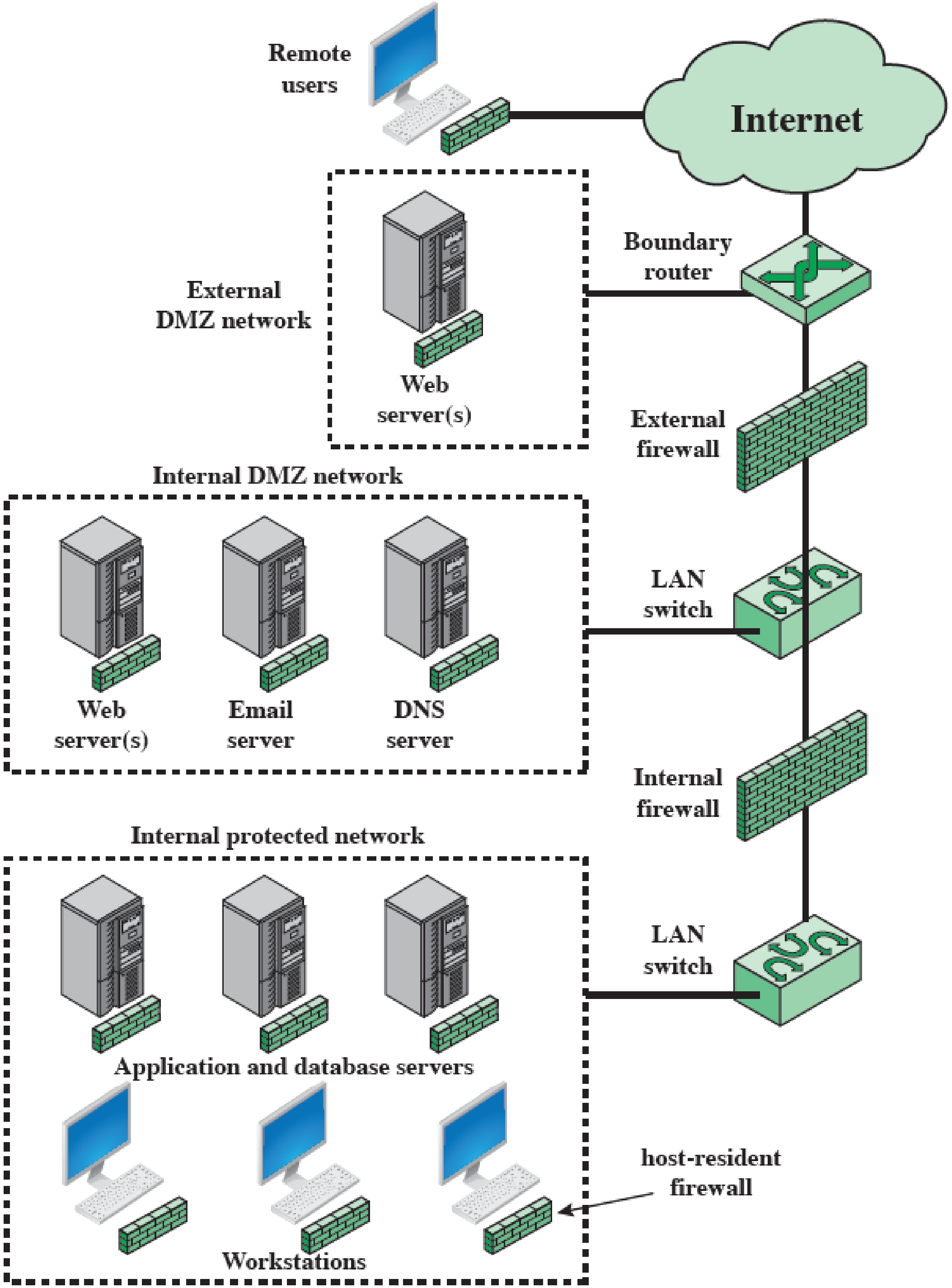
- The goal of network architecture design and implementing firewalls should be to establish a security perimeter which surrounds and protects internal information assets



- Additional security perimeters can be established around internal sub-networks in order to further strength security



Example Distributed Firewall Configuration



Source: Stallings, William. Network security essentials: Applications and standards, 6/e. Pearson Education, 2017

Acknowledgement

This material uses resources from:

- Gupta, B.B. ed., 2018. Computer and cyber security: principles, algorithm, applications, and perspectives. CRC Press.
- Stallings, William. Network security essentials: Applications and standards, 6/e. Pearson Education, 2017.
- Eric Conrad, Seth Misenar, Joshua Feldman. Eleventh Hour CISSP®: Study Guide. Syngress, Elsevier Inc. 2017.
- Verma, R.M. and Marchette, D.J., 2019. Cybersecurity Analytics. CRC Press.
- Simplilearn, 2020. Cyber Security Training For Beginners.
- Humayun, M., Niazi, M., Jhanjhi, N.Z., Alshayeb, M. and Mahmood, S., 2020. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, pp.1-19.
- Madarie, R., 2017. Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. International Journal of Cyber Criminology, 11(1).
- Akbanov, M., Vassilakis, V.G. and Logothetis, M.D., 2019. WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology.