School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

# CYBR 171 T1 2023

## Ngā whakapūtanga o Te Haumaru rorohiko
## Cybersecurity Fundamentals

**Week 8**

# Defending networks: Firewalls

# TEST #1-*In Person*

- **About the test**
  - 60 minutes long
  - Worth 25% of your final grade
  - Will take place THIS EVENING!
  - Questions will be a mix of multi-choice questions and short answer questions
  - The test covers only the materials from the first half of the course, i.e., the six weeks before the break
  - The questions will be similar to those asked in assignments and during lectures
  - Closed book, no devices, leave bags at the front
- **Time and date**
  - Tonight! Monday 1 May 2023
  - 17:30 - 18:30
- **Rooms based on surname**

# TEST #1-*Distance*

- The test is ***IN-PERSON*** unless there is a good reason for taking the online option. Hence, if you are
  - overseas,
  - outside the Wellington region,
  - or have medical issues

  Please send an email to Harith **urgently** if you need to discuss (harith.al-sahaf@ecs.vuw.ac.nz)

# Learning objectives

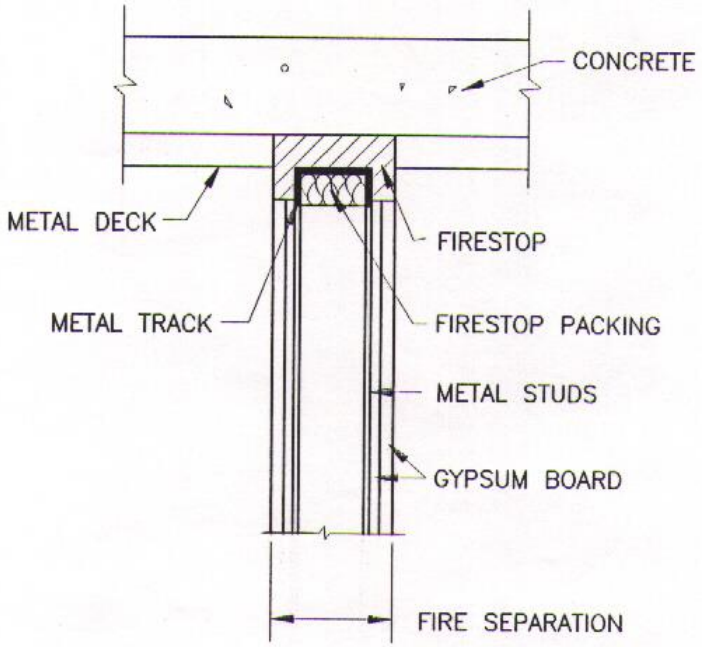
- PART 1
  - What is a firewall?
  - How do we describe firewall policies?
  - What do advanced firewalls allow?
  - How do we configure a personal firewall?
- PART 2
  - What is a VPN?
  - How do VPNs work?
- PART 3
  - Understand the risks of using VPNs.
  - Understand the difference between VPNs and TOR.

# PART 1: FIREWALL BASICS

# Firewall basics

- Building firewall:
  - Reinforced wall
  - Slows fire
  - Focus on escape

- Computer network:
  - Barrier between networks
  - Blocks dangerous communications
  - Inbound and outbound traffic




By Achim Hering - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=8267247

# Firewall basics (cont.)

# Network firewalls

- Network firewall protects local area network.

- Come in different forms.
  - Home wireless router.
  - Enterprise router.
  - Dedicated hardware firewall.

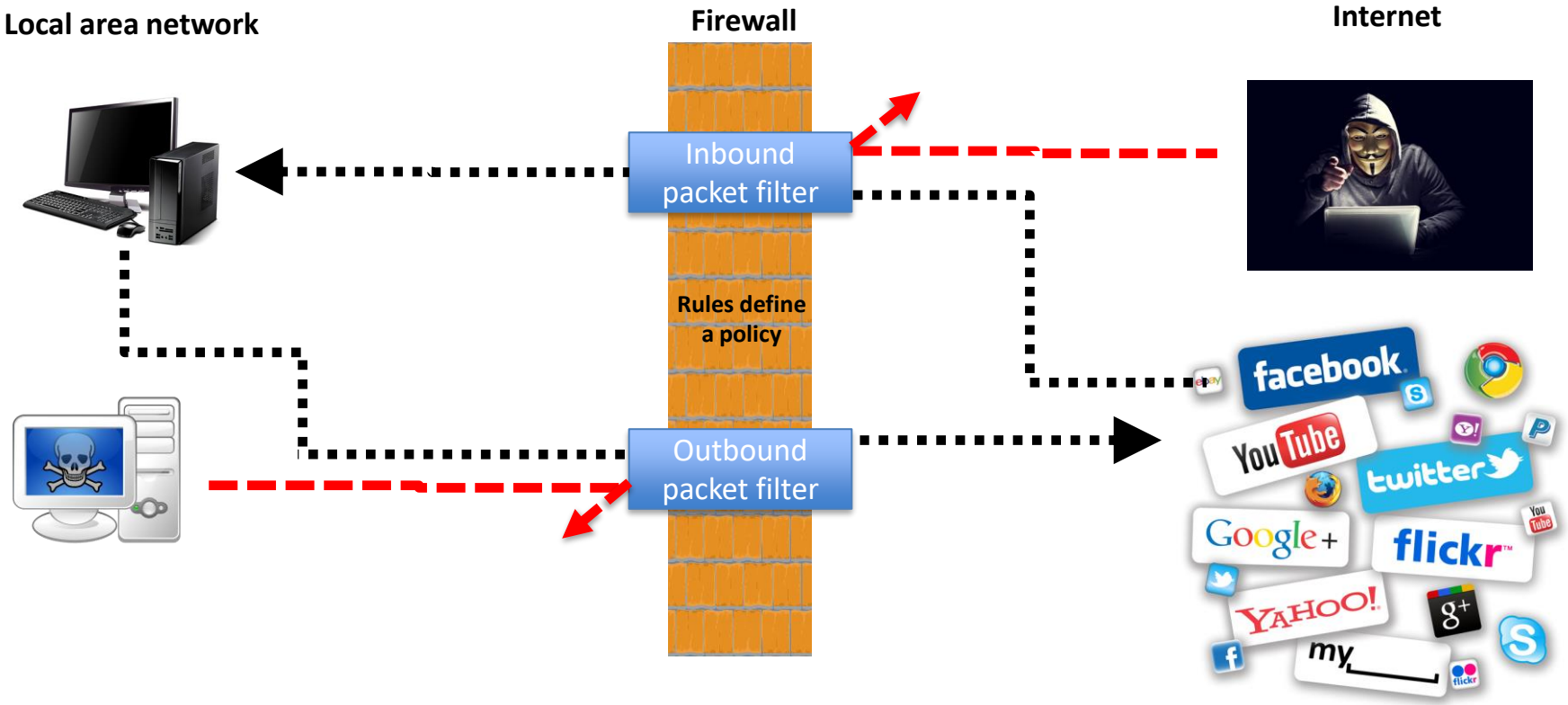
- Idea from 1988 but only implemented several years later.

Wireless router - www.netgear.com

Enterprise router - www.cisco.com

Dedicated hardware firewall - ww.watchguard.com

# How a firewall works



# Configuring a firewall policy

Policy = set of rules defining how to treat a packet.

| Direction | Source IP | Source Port | Destination IP | Destination Port | Action |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

- Direction – inbound or outbound.
- Source IP and port.
- Destination IP and port.
- Action – allow or block.

# Default policy

- Safest policy – no communication between local area network and the Internet

| Direction | Source IP | Source Port | Destination IP | Destination Port | Action |
|---|---|---|---|---|---|
| * | * | * | * | * | block |

- * = wildcard character
- Default rule for most firewalls
- Implicitly declared or always the last rule

# Example: specific machine

- Lisa's external computer with IP address W.X.Y.Z allowed access.

| Direction | Source IP | Source Port | Destination IP | Destination Port | Action |
|---|---|---|---|---|---|
| Inbound | W.X.Y.Z | * | * | * | allow |
| Outbound | * | * | W.X.Y.Z | >1023 | allow |
| * | * | * | * | * | block |

1. Allows any packet from W.X.Y.Z to enter the local area network.
2. Allows any reply packet from the local area network to reach only a machine with the IP address W.X.Y.Z located in the Internet (assumes that any reply packet has dynamic port > 1023).
3. Drops any packet not matching rule 1 or 2.

# Example: specific service

- Internal users are allowed access to the web.

| Direction | Source IP | Source Port | Destination IP | Destination Port | Action |
|---|---|---|---|---|---|
| Outbound | * | * | * | 80 | allow |
| Outbound | * | * | * | 443 | allow |
| Inbound | * | * | * | > 1023 | allow |
| * | * | * | * | * | block |

- Rules 1,2: allows any http (80) or https (443) request from local area network to reach any machine on the Internet.
- Rule 3: allows any machine on the Internet to reach any machine on the local area network listening on a dynamic port > 1023.
- Rule 4: block all other packets.
- NOTE: this policy could be made tighter still.

# Advanced firewalls

- More **complex** rules:
  - Protocol (TCP, UDP or ICMP).
  - New or existing connection.
  - Application sending or receiving packets.
  - Silently block or close the connection.
  - Deep packet inspection (code or data payloads).

- Example advanced policies:
  - Block application using excessive bandwidth.
  - Restrict traffic to connections initiated by a specific machine.
  - Prevent traffic containing malware or sensitive information.

# Personal firewalls

- Part of the operating system.
- Additional protection to network firewall.
- Ideal for laptops that connect to different networks.
- User specifies the policy.
- Administrator privileges to manage.
- Company devices often managed centrally.
- ***Malware and attackers usually try to turn the firewall off.***


**Firewall & network protections: Keep unwanted online traffic out**


# PART 2: VIRTUAL PRIVATE NETWORKS (VPNs)

# Virtual Private Networks (VPNs)

- Local network bit like a castle.
- Safe behind the walls.
- Outside the castle are dangers.
- Risks when travel between them.
- Similar to when we use the Internet.

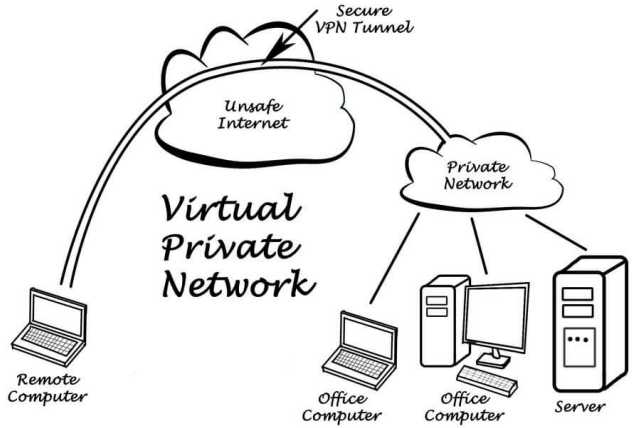
https://www.travelzoo.com/blog/8-fairy-tale-esque-castles-world/

# Need for VPNs

- Many physical locations.
- Mobile workforce.
  - Sales teams.
  - People working from home.
- Too expensive for a private network.
- VPN = private network across untrusted network
  - i.e. the Internet

# Implementing a VPN

- VPN client
  - Software installed on client.
  - Connects user to remote local area network.
- VPN server
  - Part of dedicated network device.
  - Authenticates users and routes traffic.
  - Example: firewall or VPN concentrator.
- Tunnel:
  - Established between client and server.
  - ***Treats the client as if it is on the local area network.***




http://bestwirelessroutersnow.com/what-vpn-concentrator/

# Securing the tunnels

- Encryption:
  - Performed by software.
  - Early version proprietary.
  - Now public standards.
- Authenticity and integrity:
  - Hashes.
  - Digital signatures.
  - Message authentication codes (MACs)
- MACs like digital signatures but use symmetric encryption.


# PART 3: SECURITY RISK OF VPNs
# VPN VS. TOR

# Security risks of VPNs

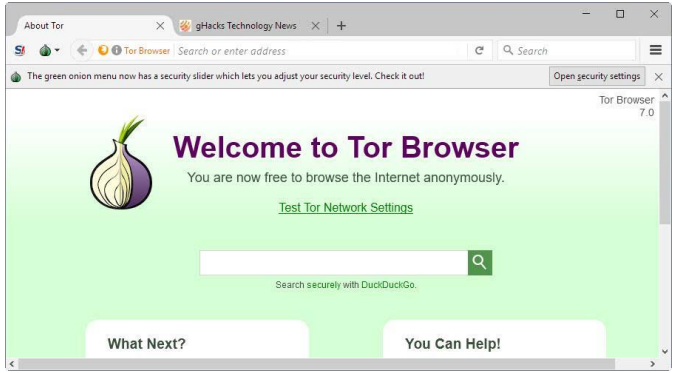
- Security of remote machines:
  - Direct route into corporate network.
  - Bypasses the firewall.
- Security of VPN implementation:
  - Can be flawed.
  - Microsoft implementation had vulnerabilities in 1998.
- Security of network availability:
  - Cannot guarantee reliability because relies on the Internet.

# VPNs for everybody

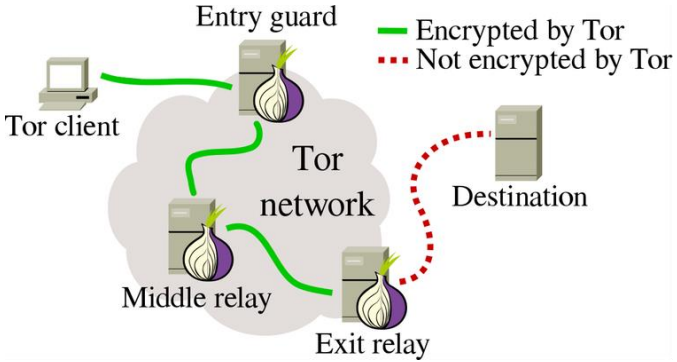
- Protect yourself when using public wifi.
- Appear to come from a different country.
  - Avoid Geoblocking, led to cease and desist notices to NZ ISP
  - Access blocked sites (for example, in China).
- Provide limited anonymity:
  - Easy to identify VPN servers.
  - Data may be seized by law enforcement or government agencies.

# TOR

- TOR project was started in 1995 by US Naval Research Lab.
- Now independent not-for-profit.
- Onion routing hides your exit point on the network.
  https://video.link/w/GYQfc
- Idea is to help ordinary people and activists:
  - Arab spring 2010-
  - Edward Snowden 2013




https://www.torproject.org/about/history/



# What is next

- Test 1 5.30pm today
- Intrusion Detection Systems (IDS)
- Honeypot Systems
- Thursday guest lecture Ben Creet NCSC
- Lab 3 due Sunday 7 May 11.59pm
- Assignment 2 will be released by later tonight