Computer and Network Security

Lecture 17: WWW & Web Attacks

COMP-5370/6370
Fall 2025

Firewalls

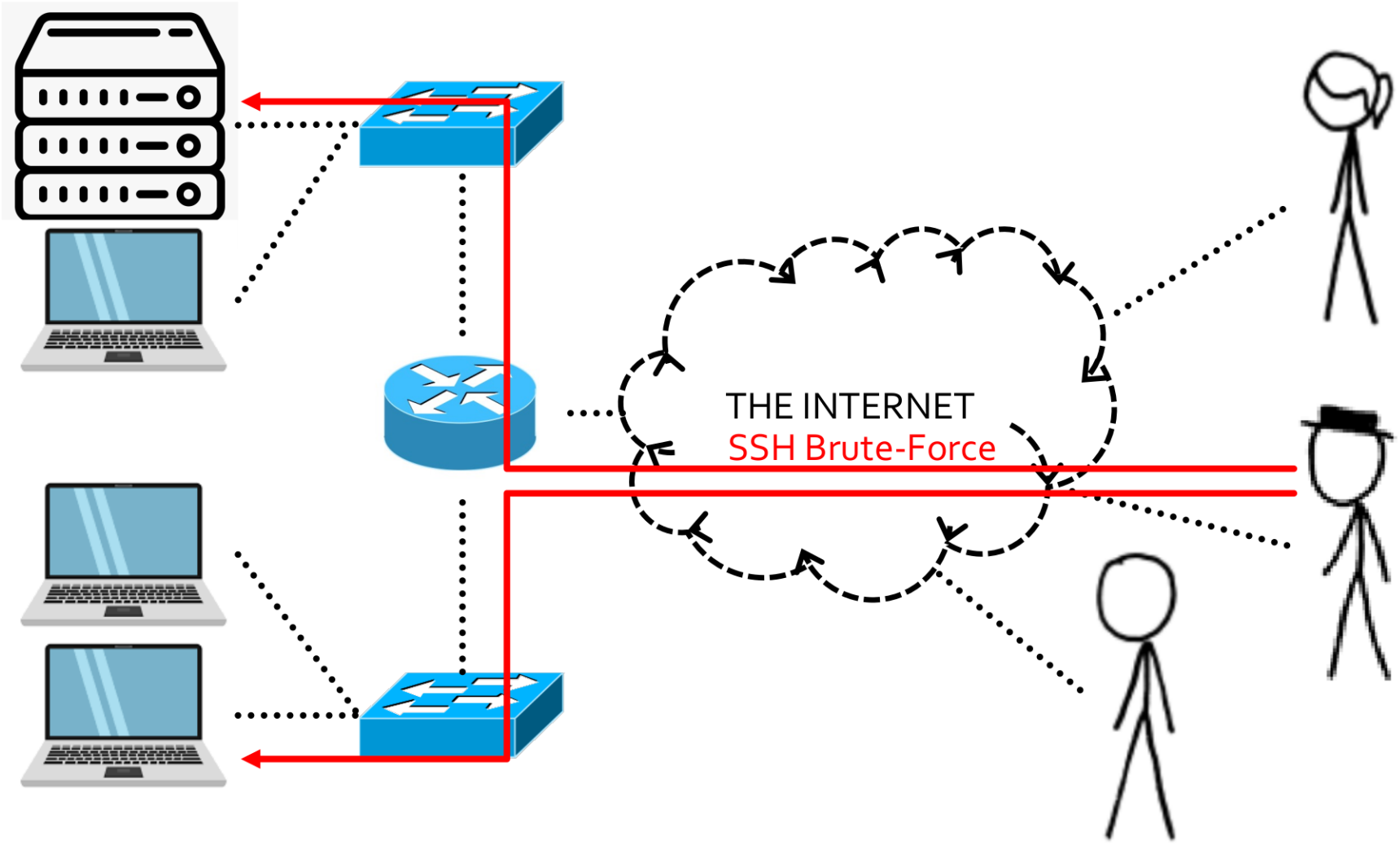
A **firewall** is a generic name for a network-level defense tactic that blindly applies a rule-based policy to network traffic.

- Operate on L3 and L4 (IPs and TCP/UDP)
- Logically, the rules are straight-forward
  - **DO** allow port 80 (HTTP)
  - **DON'T** allow port 22 (SSH)
  - **DON'T** allow port 21 (FTP) **UNLESS** comes from <*remote office IP*>

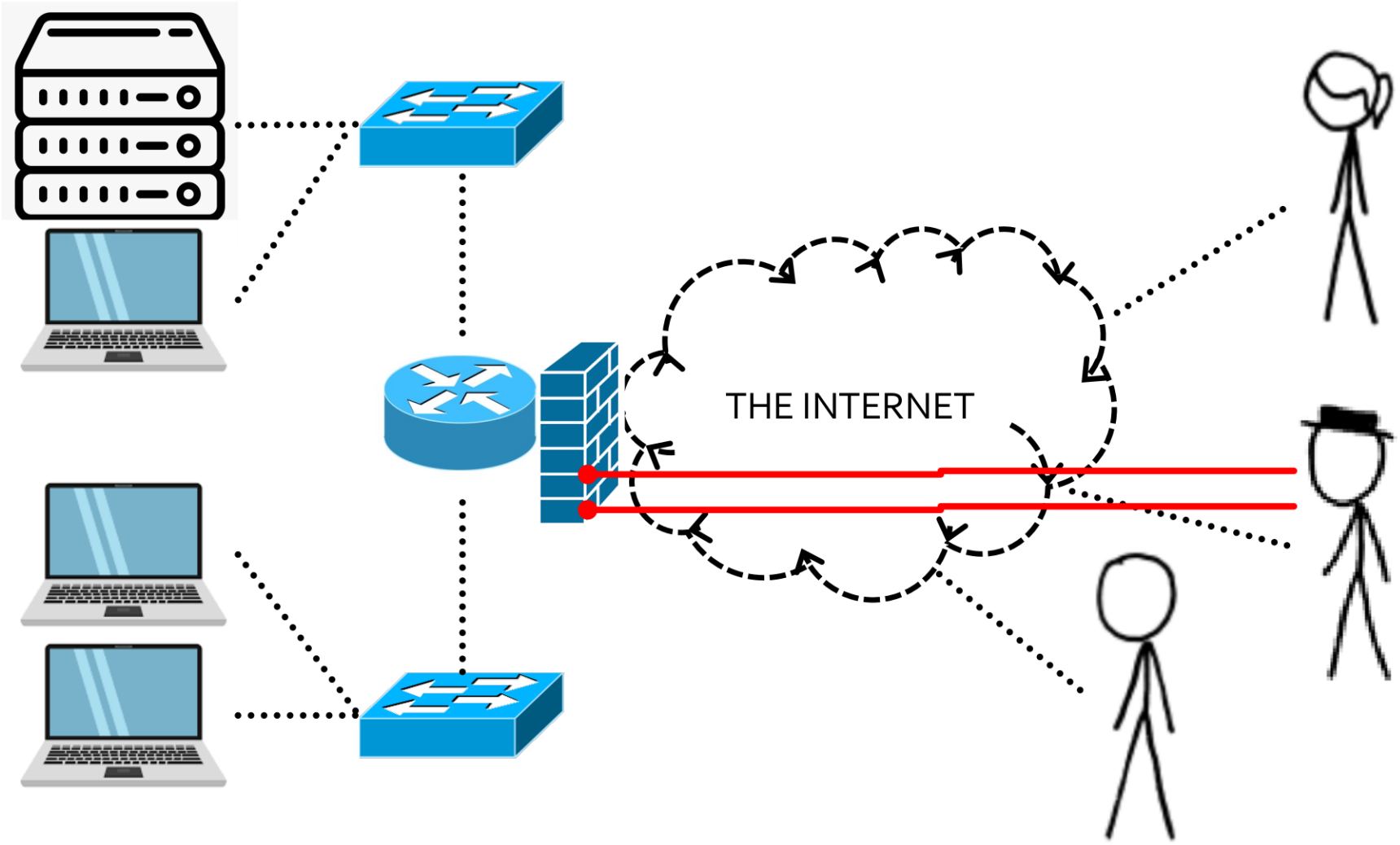
Firewall Implementations

- Network-based
  - Runs as own device in front of many devices
  - **PRO:** Single management point
  - **CON:** Complex rules for complex networks

External Attacks



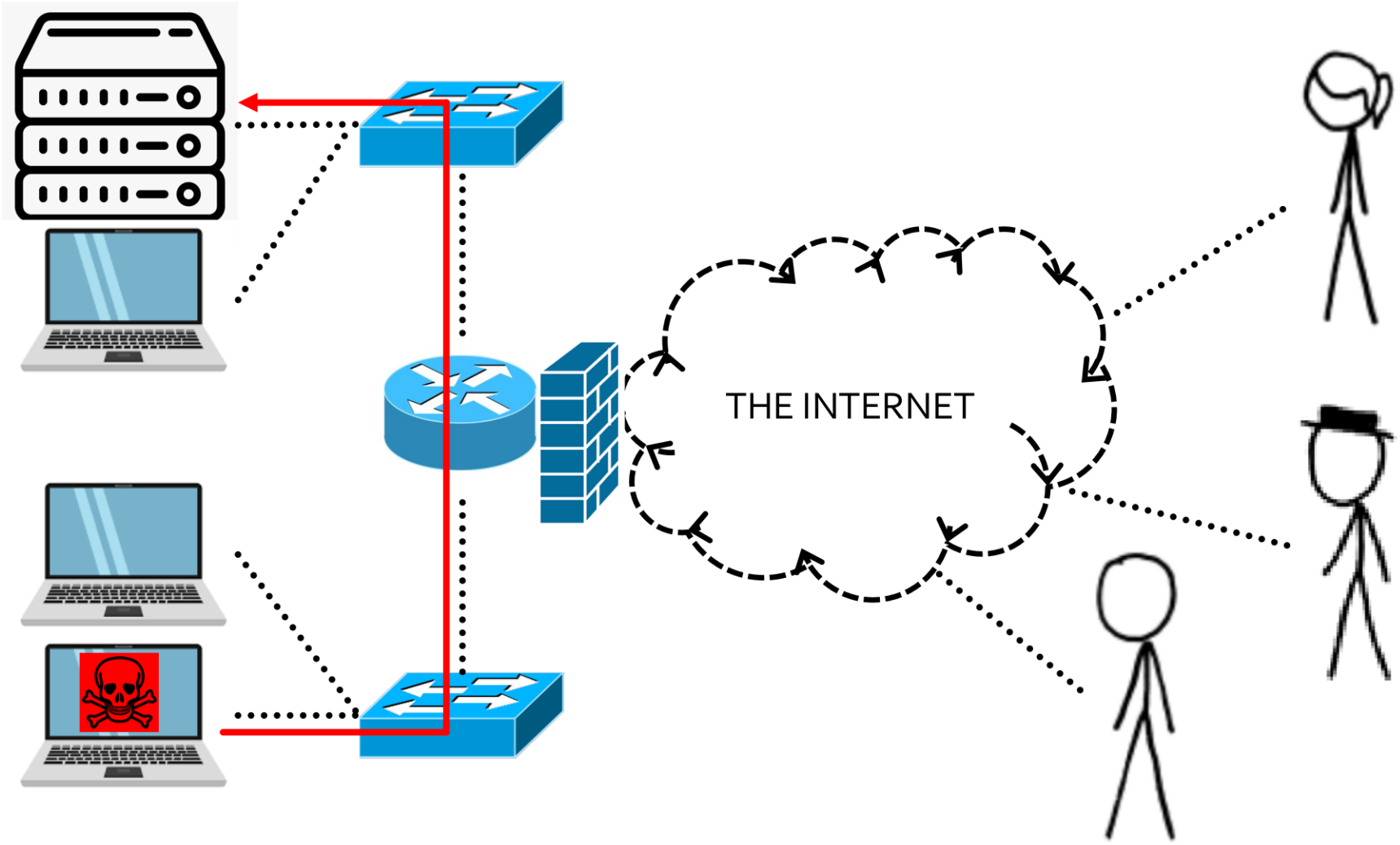
External Attacks



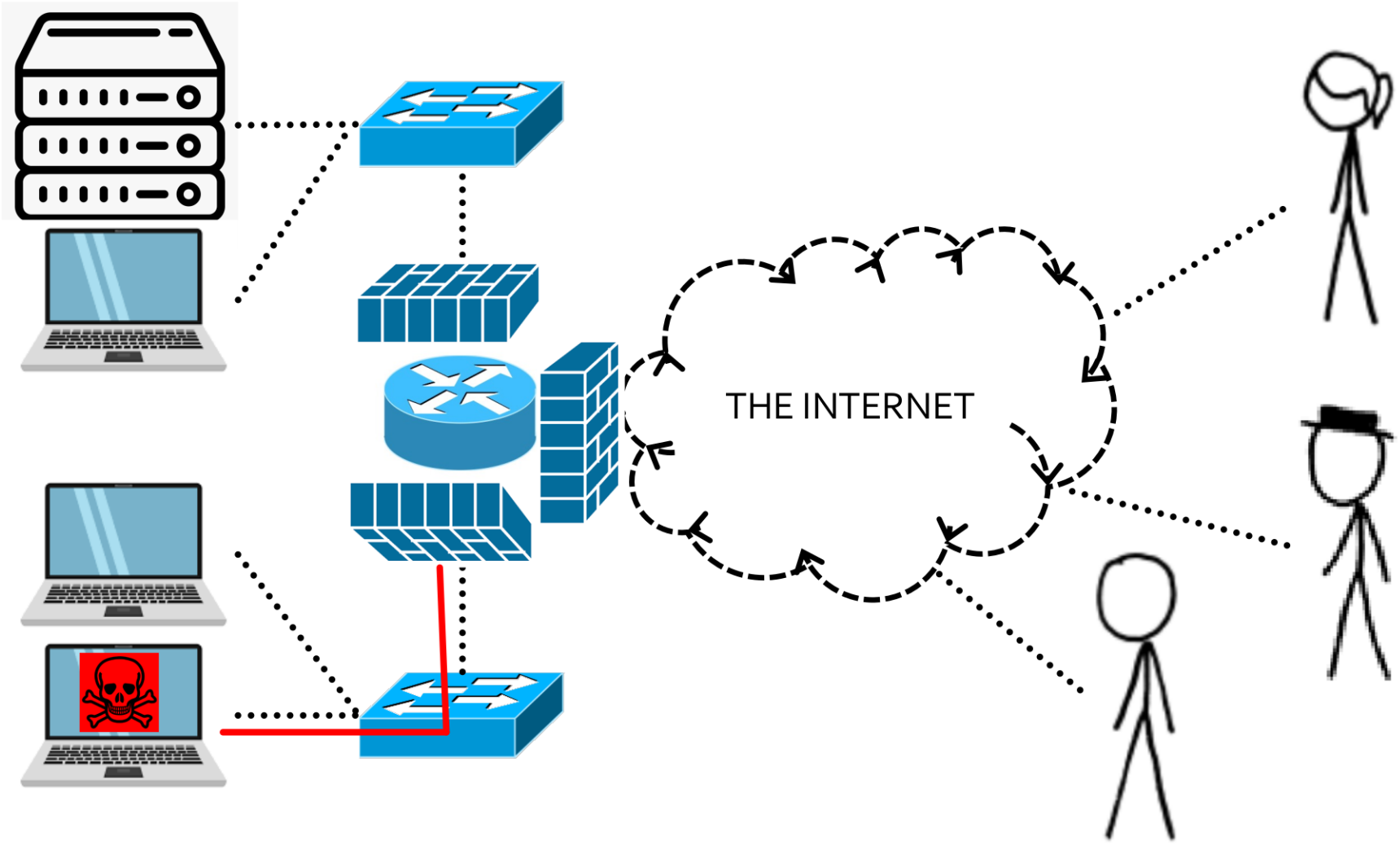
Firewall Implementations

- Network-based
  - Runs as own device in front of many devices
  - **PRO:** Single management point
  - **CON:** Complex rules for complex networks
  - **CON:** Stationary, single view-point

Internal Attacks



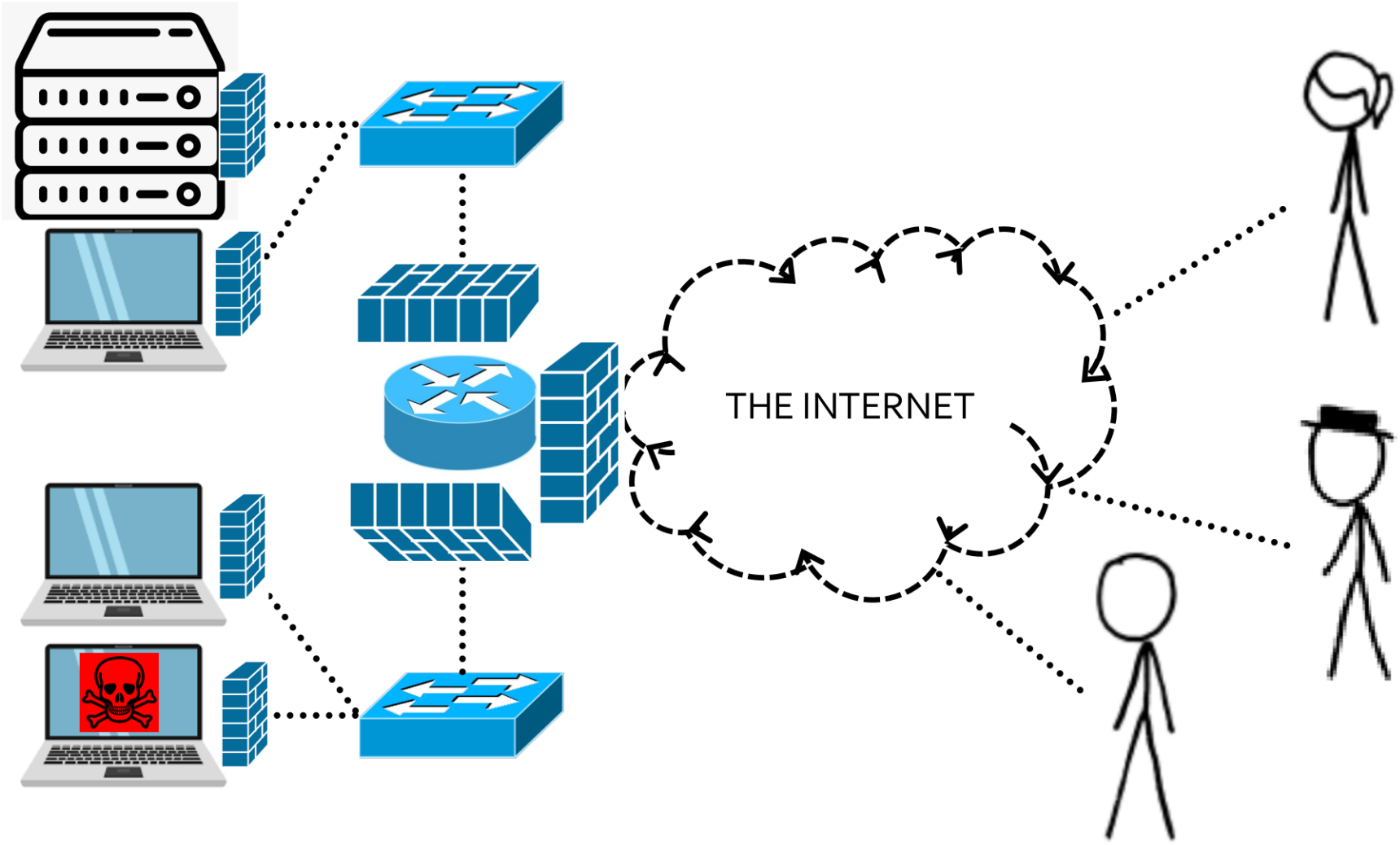
Block Internal Attacks



Firewall Implementations

- Network-based
  - Runs as own device in front of many devices
  - **PRO:** Single management point
  - **CON:** Complex rules for complex networks
- Host-based Firewalls
  - Runs on each individual devices for itself
  - **PRO:** Devices can have different rule sets
  - **CON:** More to manage and update

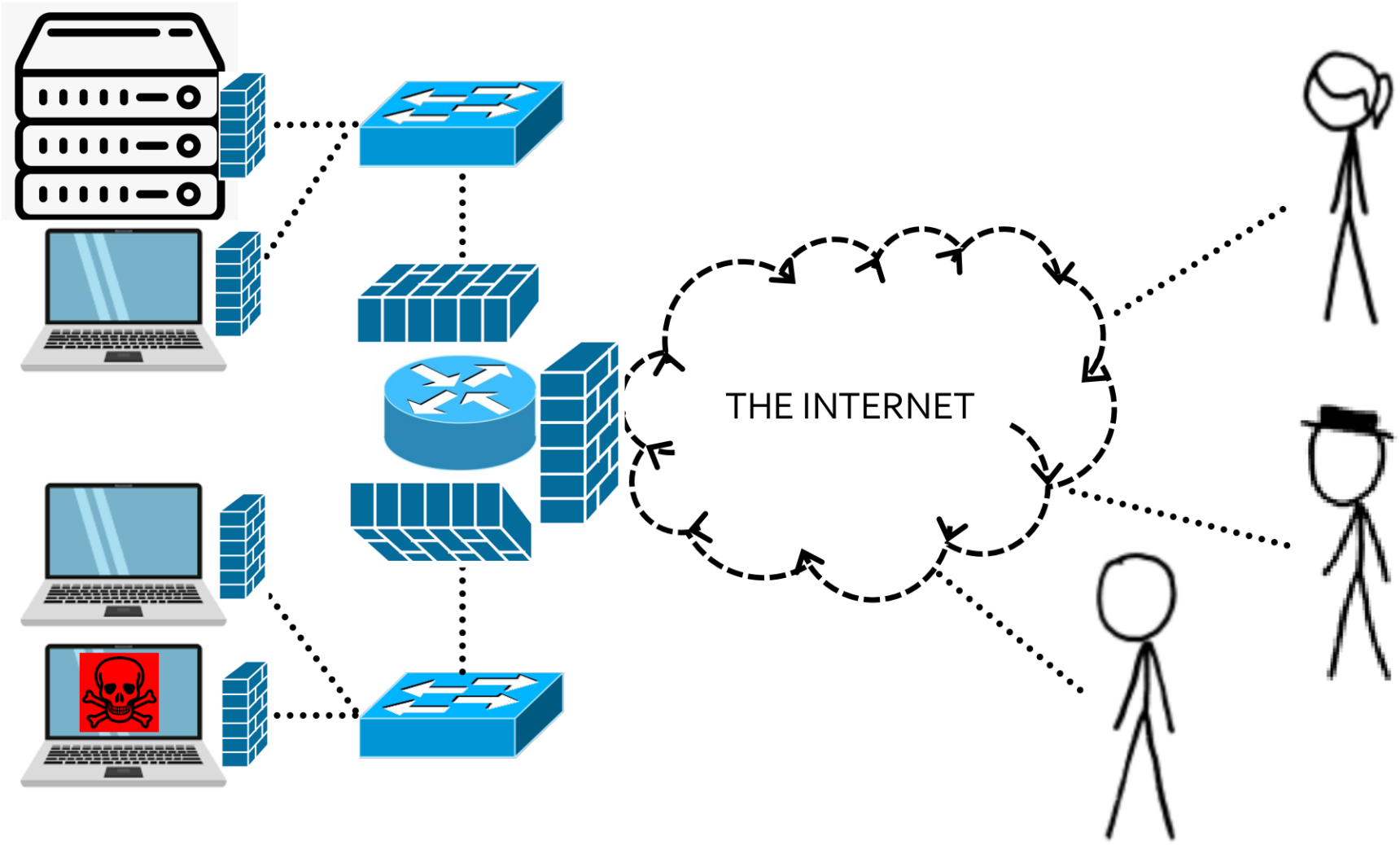
Not-Awful Network Topology



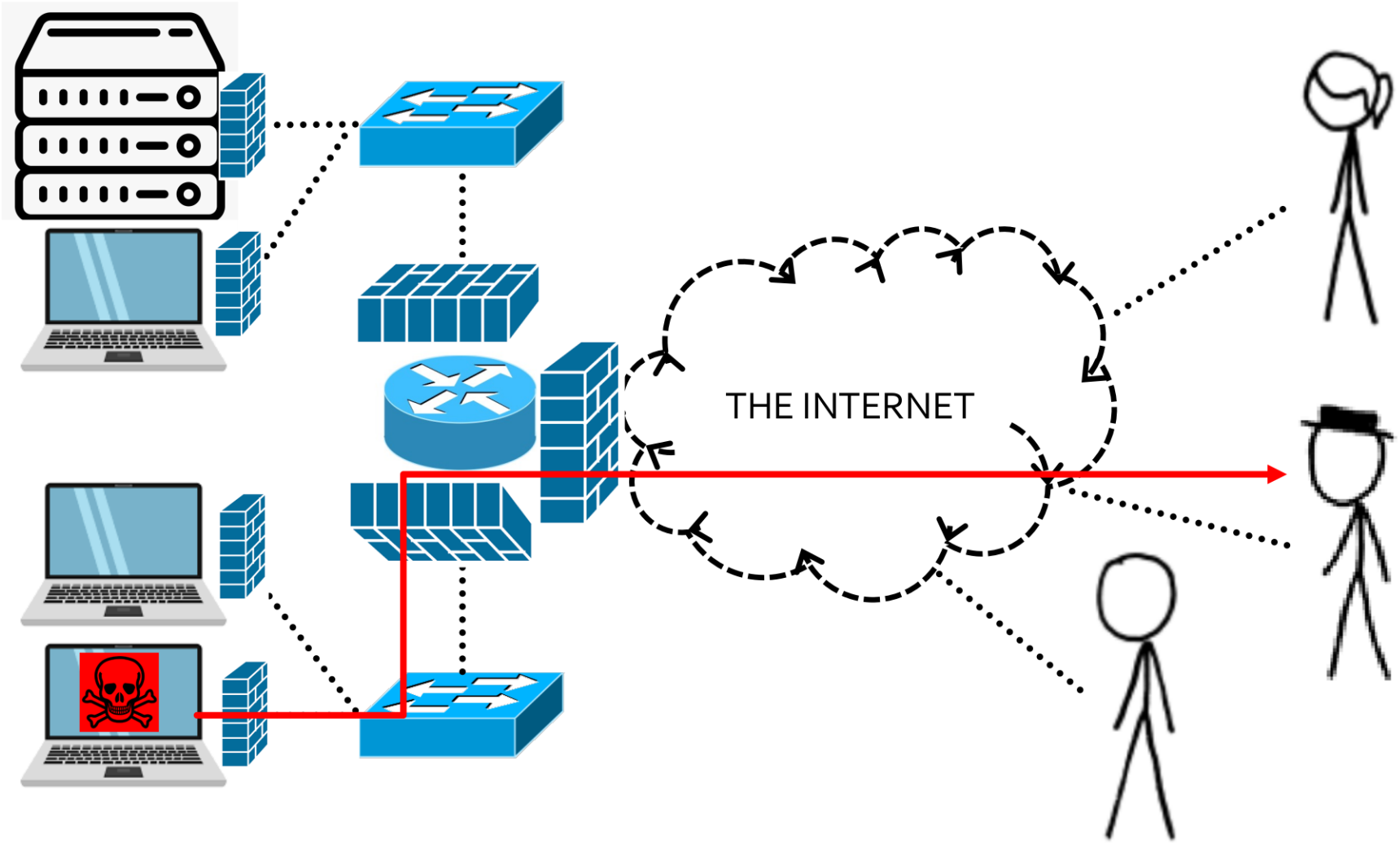
Firewall Options in 2025

- Most network devices have some sort of built-in firewall
  - Including most consumer-grade equipment
- All standard OSes have built-in firewalls
  - Linux – iptables / UFW / pf / nftables
  - Windows – Windows Firewall
  - macOS – Firewall
- **IoT and embedded devices often lack ☹**
  - Rely on network-level to handle

Not-Awful Network Topology



Not-Awful Network Topology

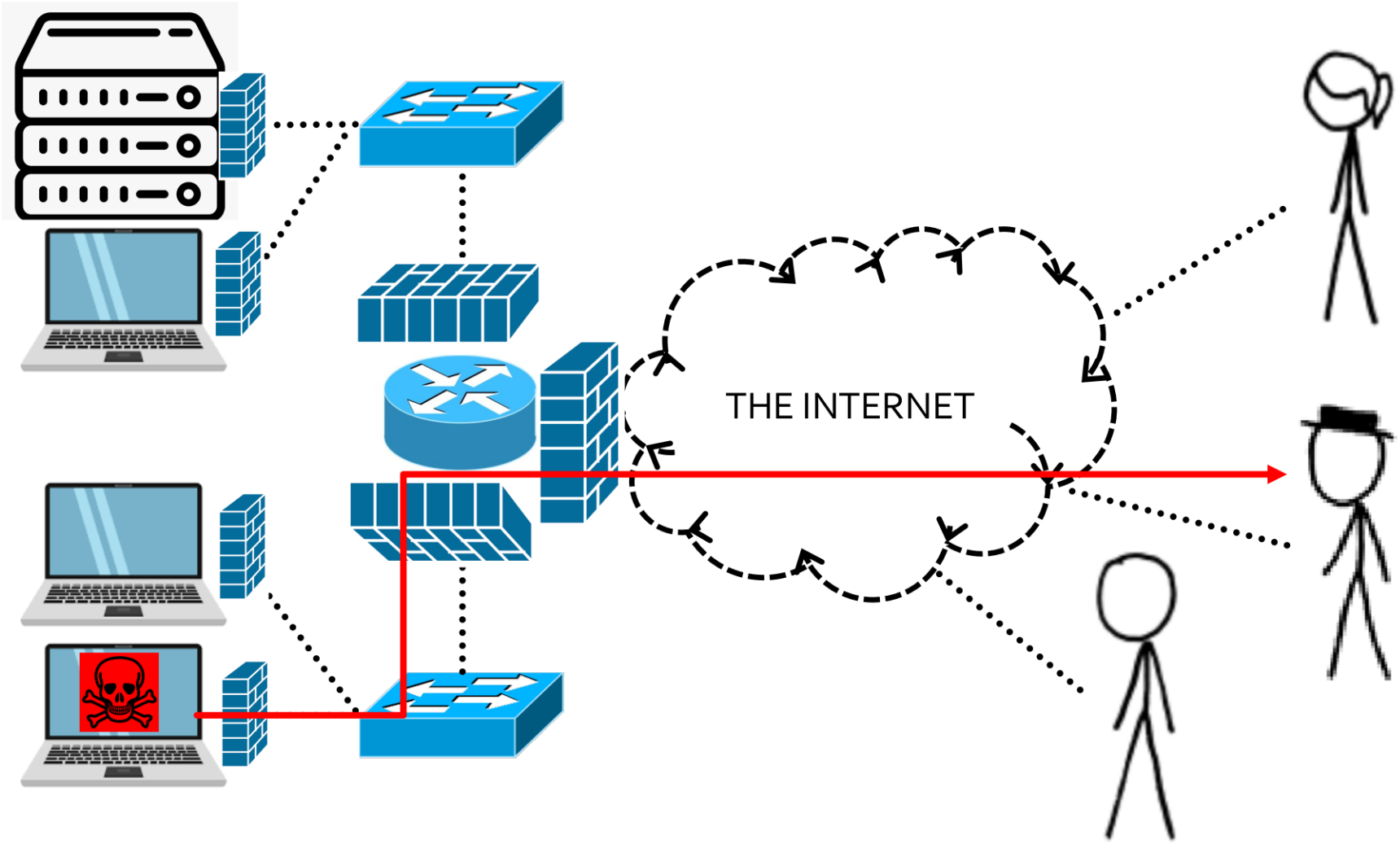


Intrusion Detection System (IDS)

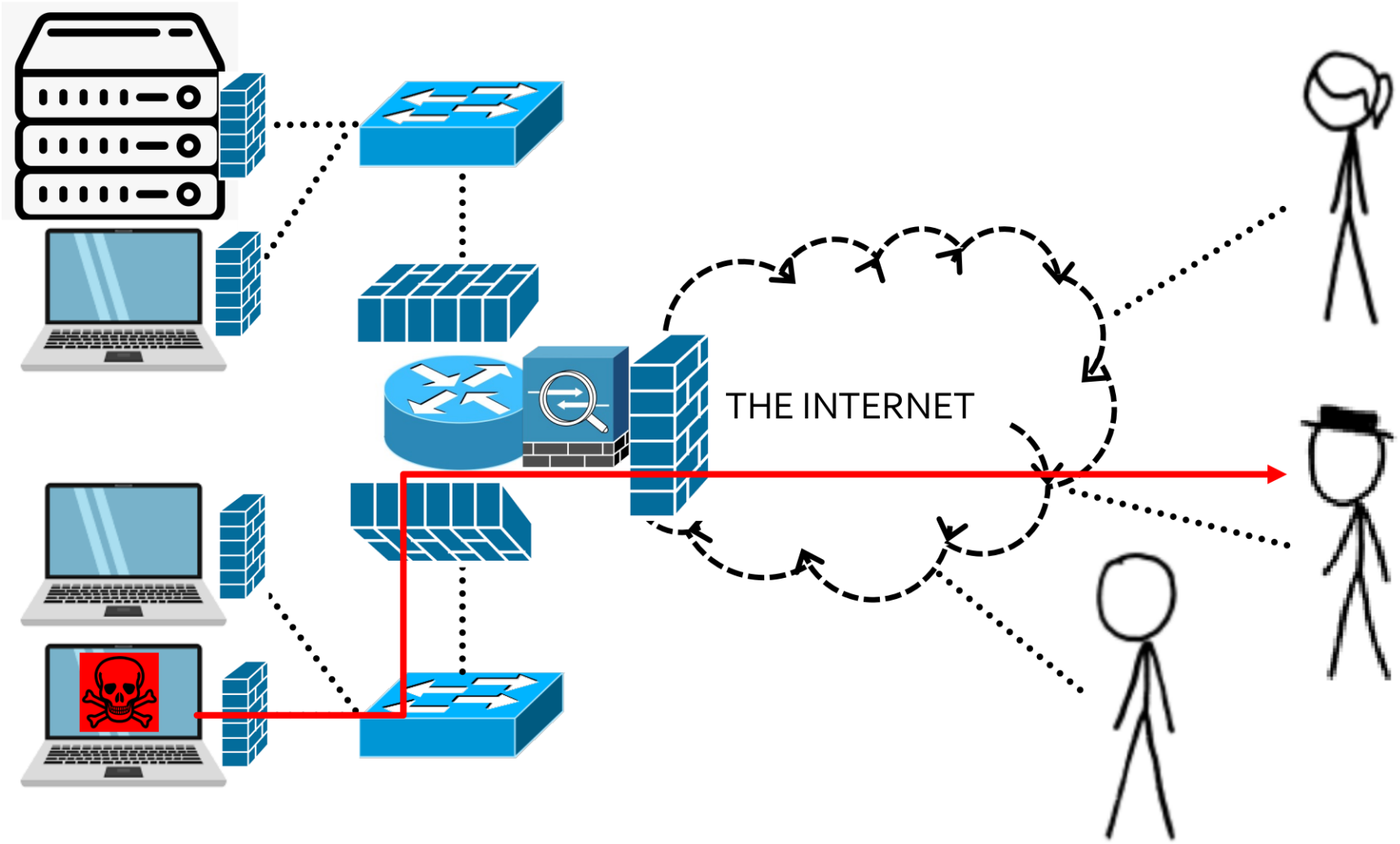
An **Intrusion Detection System (IDS)** is a network *monitoring* component that is able to *watch* for signs of maliciousness.

- Capable of granular and complex rules
  - Beyond L3/L4 headers
  - “Deep Packet Inspection” (DPI)

Not-Awful Network Topology



Not-Awful Network Topology

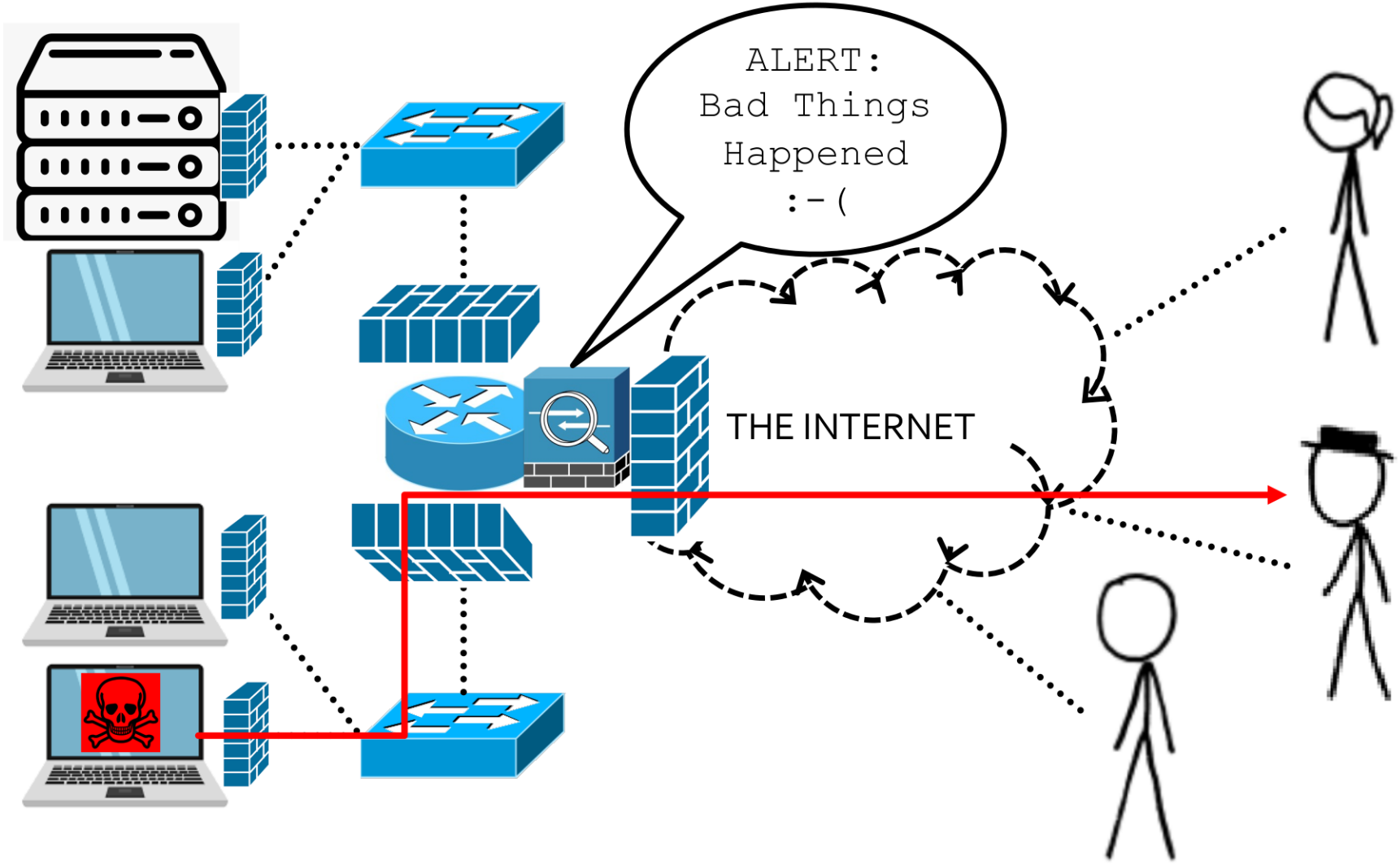


Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a network *monitoring* component that is able to *watch* for signs of maliciousness.

- Capable of granular and complex rules
  - Beyond L3/L4 headers
  - “Deep Packet Inspection” (DPI)
- Capable of pattern/regex matching
- Capable of searching for multi-flow patterns

Not-Awful Network Topology



Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a network *monitoring* component that is able to *watch* for signs of maliciousness.

- Capable of granular and complex rules
  - Beyond L3/L4 headers
  - “Deep Packet Inspection” (DPI)
- Capable of pattern/regex matching
- Capable of searching for multi-flow patterns

Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a network ***monitoring*** component that is able to ***watch*** for signs of maliciousness.

- Capable of granular and complex rules
  - Beyond L3/L4 headers
  - “Deep Packet Inspection” (DPI)
- Capable of pattern/regex matching
- Capable of searching for multi-flow patterns

Intrusion Prevention System (IPS)

An **Intrusion Prevention System (IPS)** is a type of IDS which is able to actively block maliciousness when found.

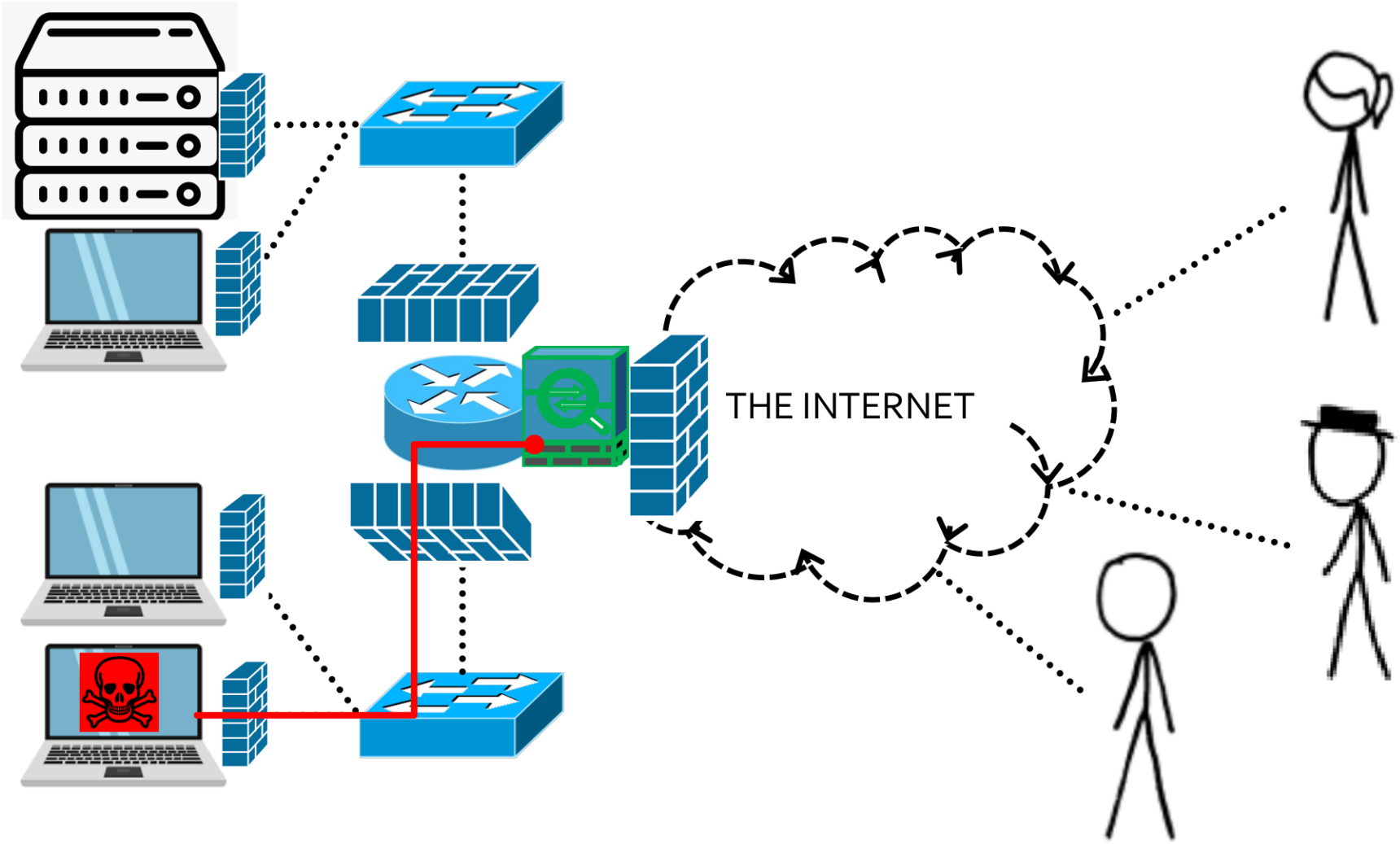
- Capable of granular and complex rules
  - Beyond L2/L3 (TCP/IP) headers
  - “Deep Packet Inspection” (DPI)
- Capable of pattern/regex matching
- Capable of searching for multi-flow patterns

Intrusion Prevention System (IPS)

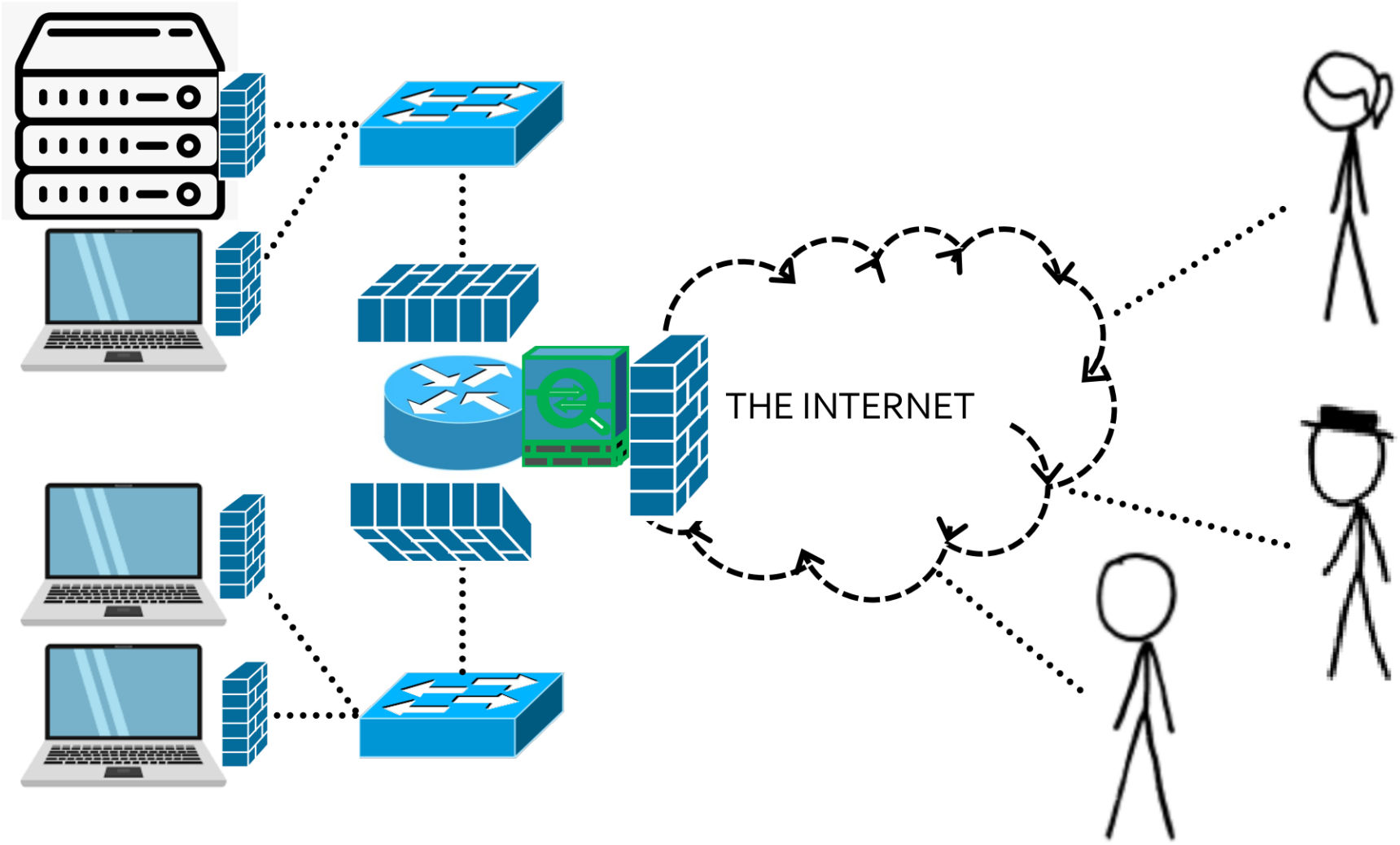
An **Intrusion Prevention System (IPS)** is a type of IDS which is able to **actively block** maliciousness when found.

- Capable of granular and complex rules
  - Beyond L2/L3 (TCP/IP) headers
  - “Deep Packet Inspection” (DPI)
- Capable of pattern/regex matching
- Capable of searching for multi-flow patterns

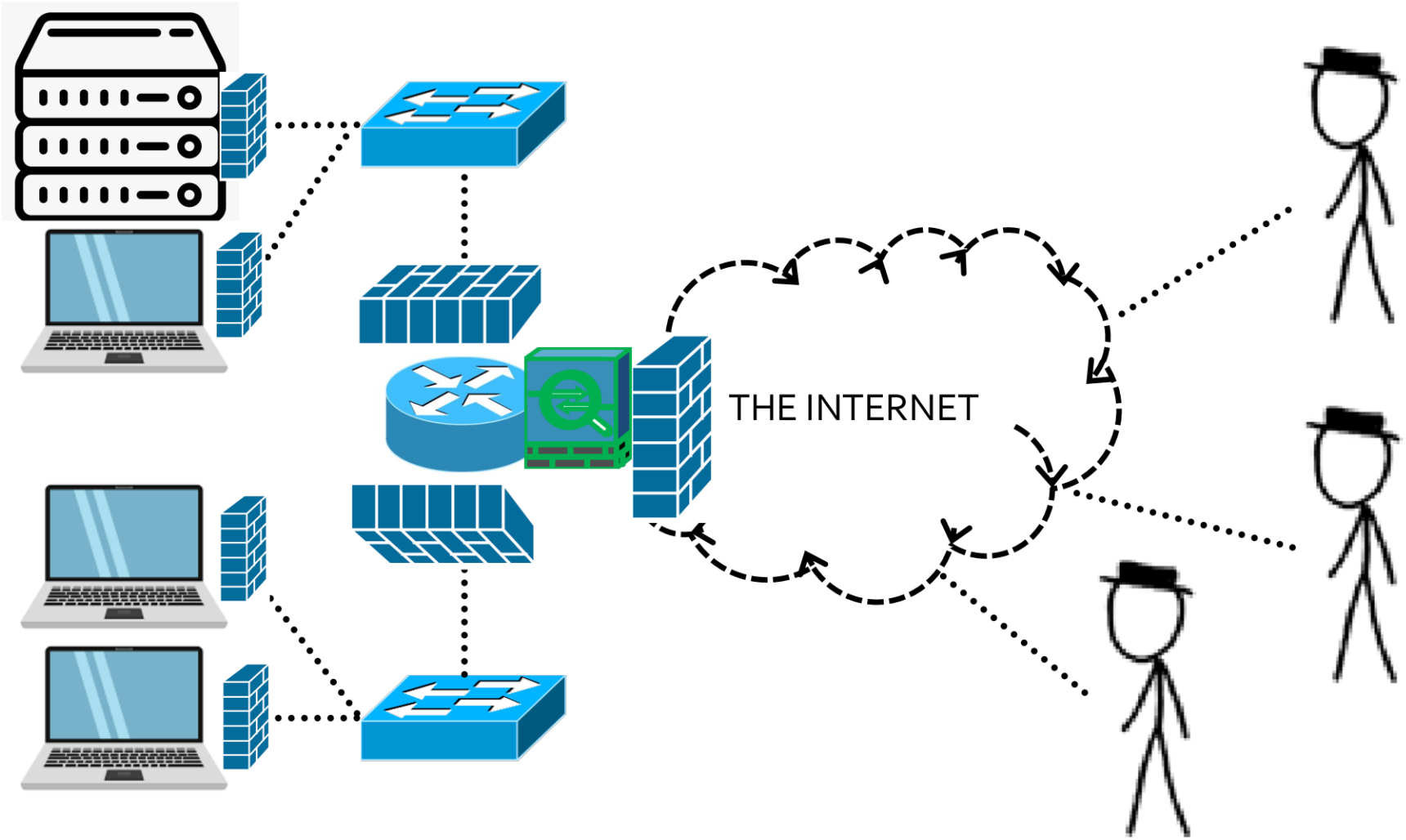
Not-Awful Network Topology



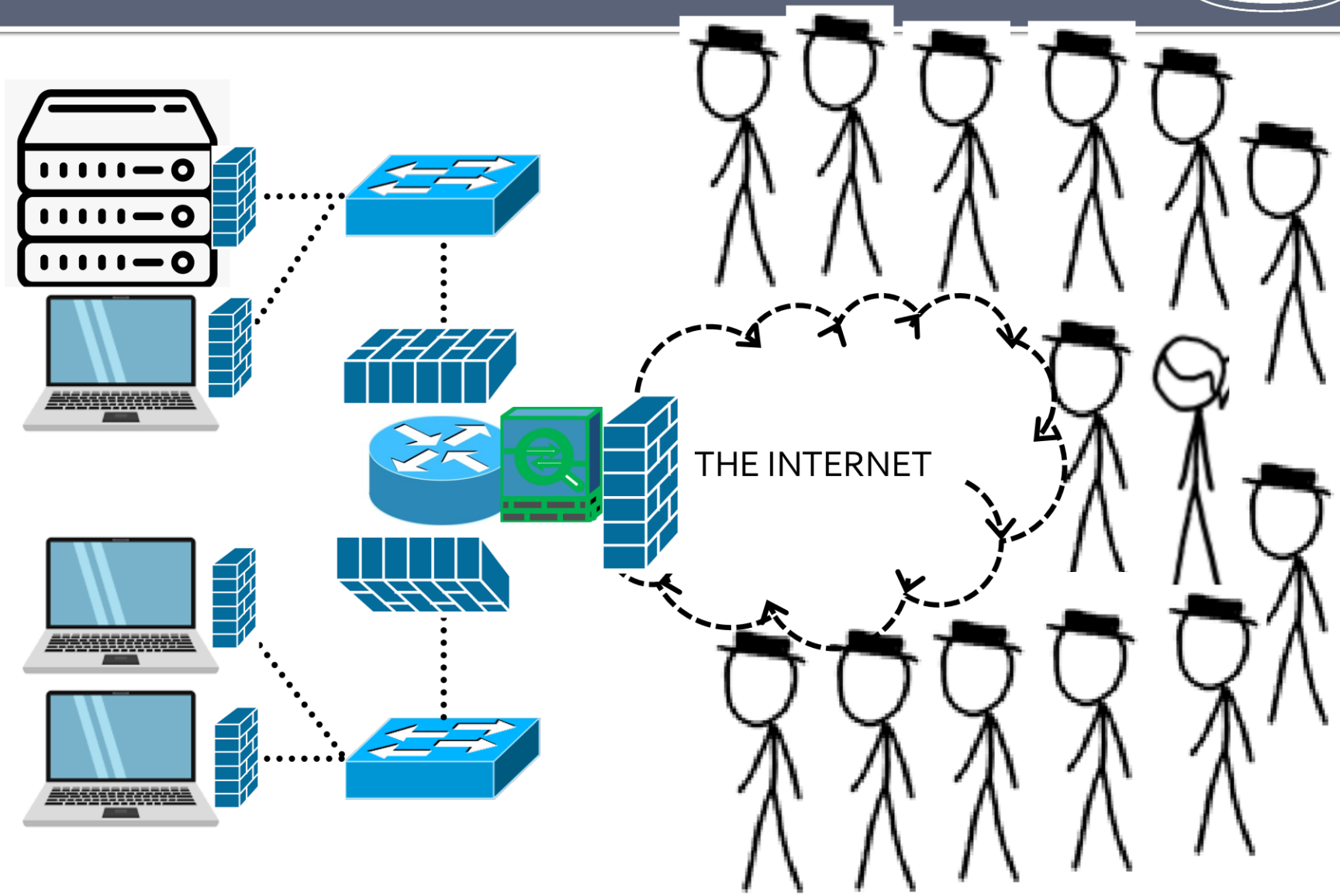
OK Network Topology



OK Network Topology



OK Network Topology

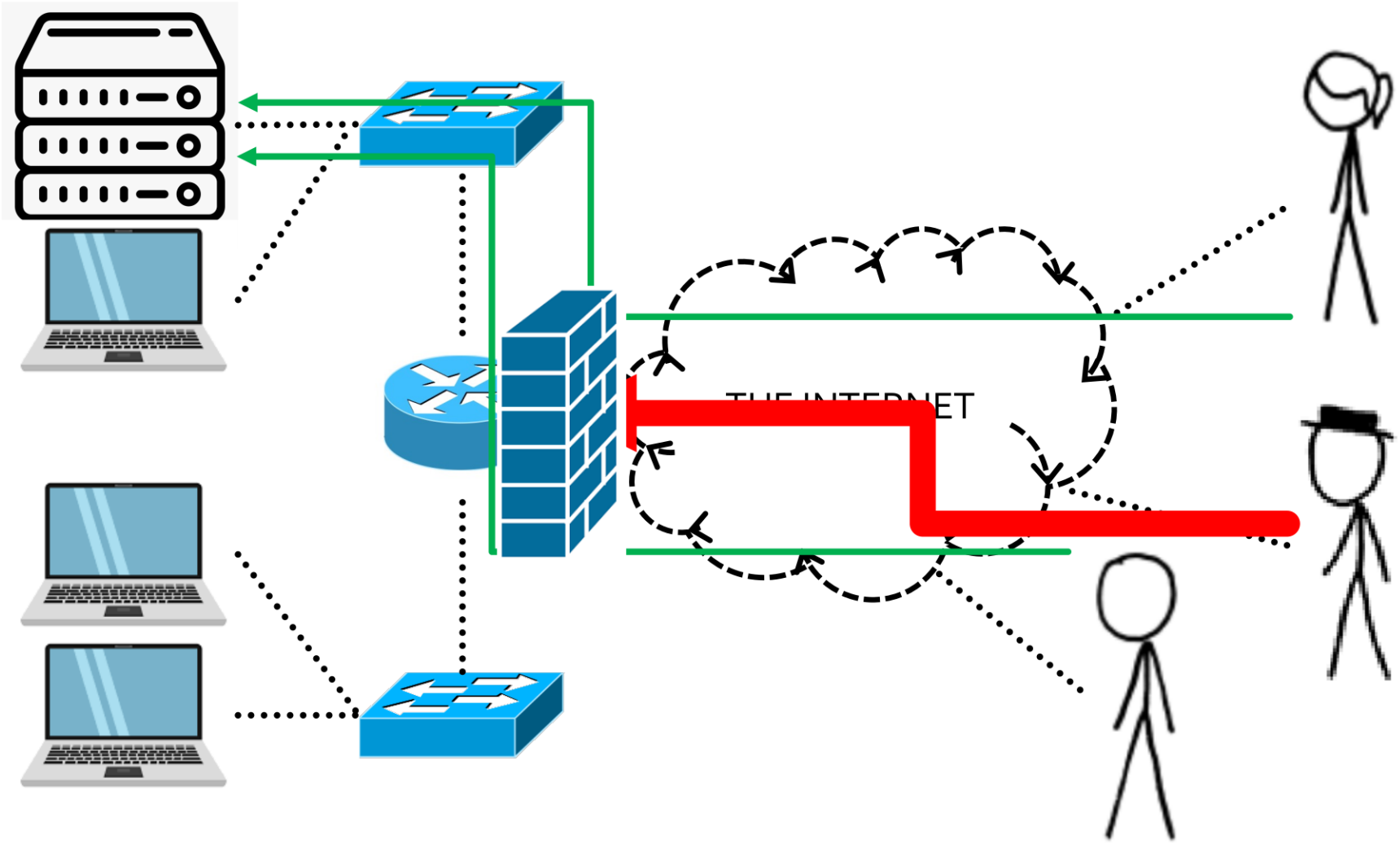


Denial of Service (DoS) Attacks

Denial of Service (DoS) is a type of attack which desires to prevent legitimate users from accessing a service.

- Usually based on an "asymmetric" tradeoff that favors the attacker
  - Attacker's cost is very small but defender's cost is very high

Asymmetric Tradeoffs

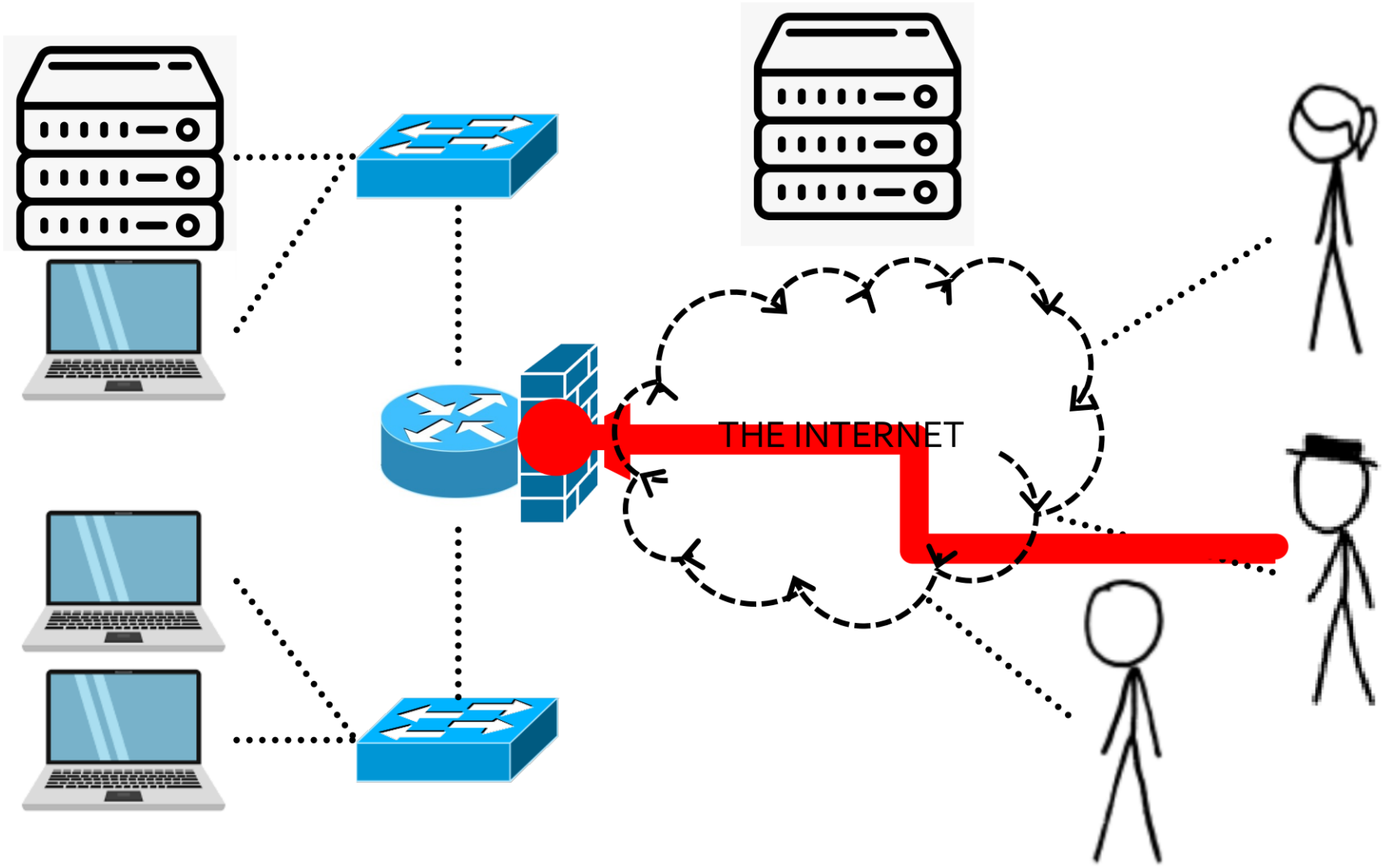


Denial of Service (DoS) Attacks

Denial of Service (DoS) is a type of attack which desires to prevent legitimate users from accessing a service.

- Usually based on an "asymmetric" tradeoff that favors the attacker
  - Attacker's cost is very small but defender's cost is very high
- Come in many different varieties

Traffic Floods

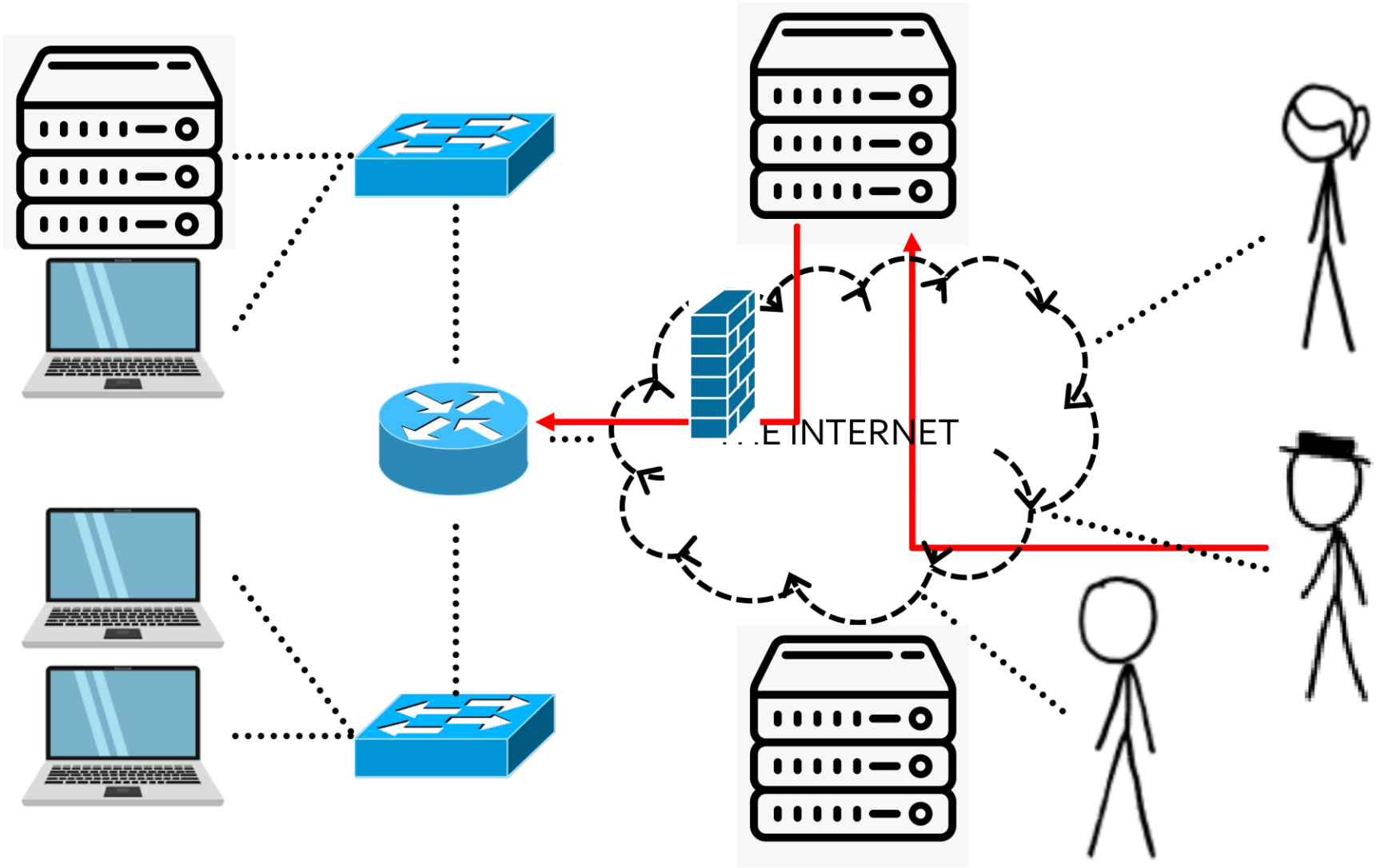


Reflection Attacks

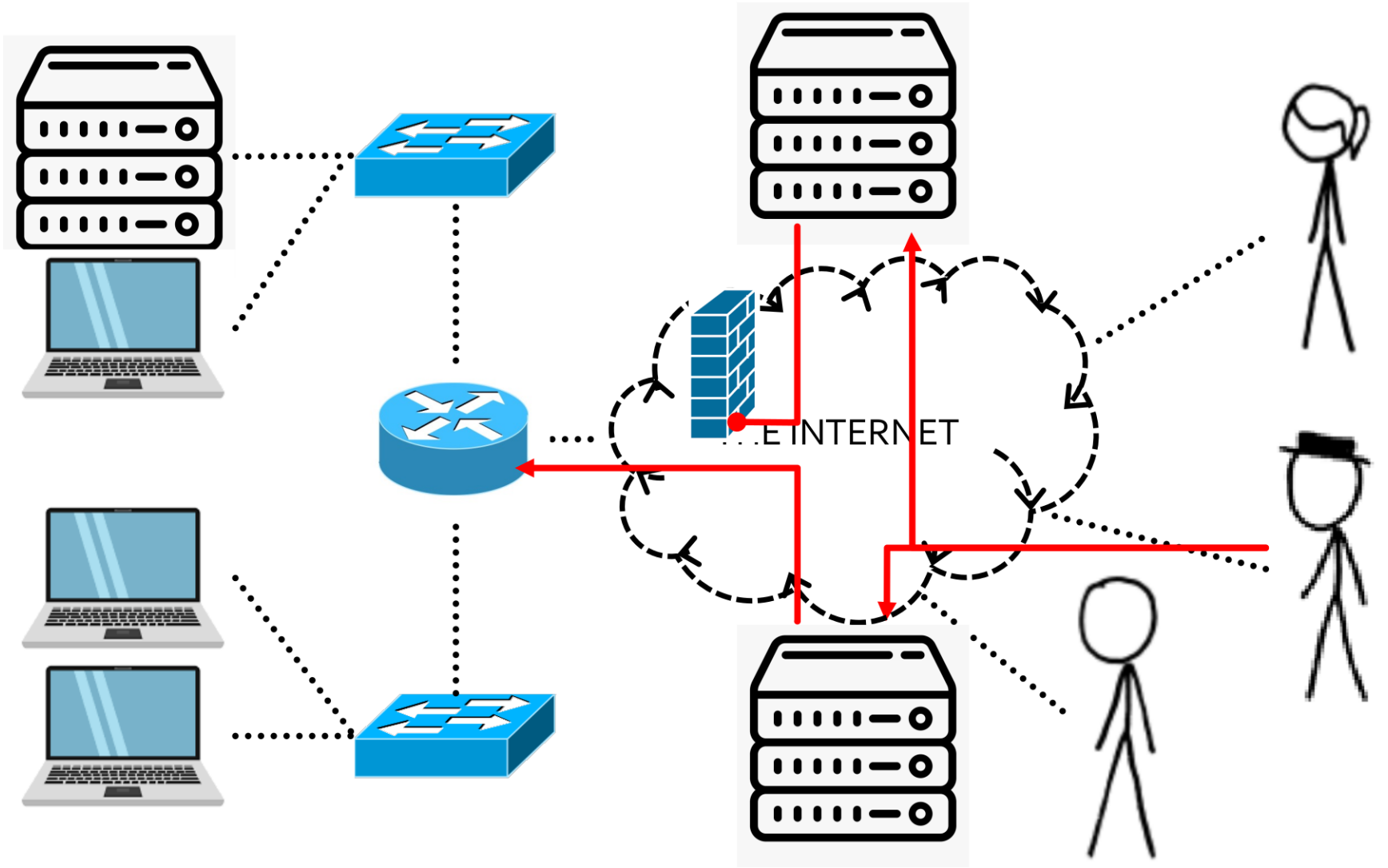
Reflection Attacks are a type of network attack where the traffic is “bounced” through a third-party in order to hide its source.

- Usually relies on forging the source IP
  - Causes the 3P to send traffic to the victim
- Victim can block the source-IP (bouncing server) but never see the actual attacker

Reflection Attacks



Reflection Attacks

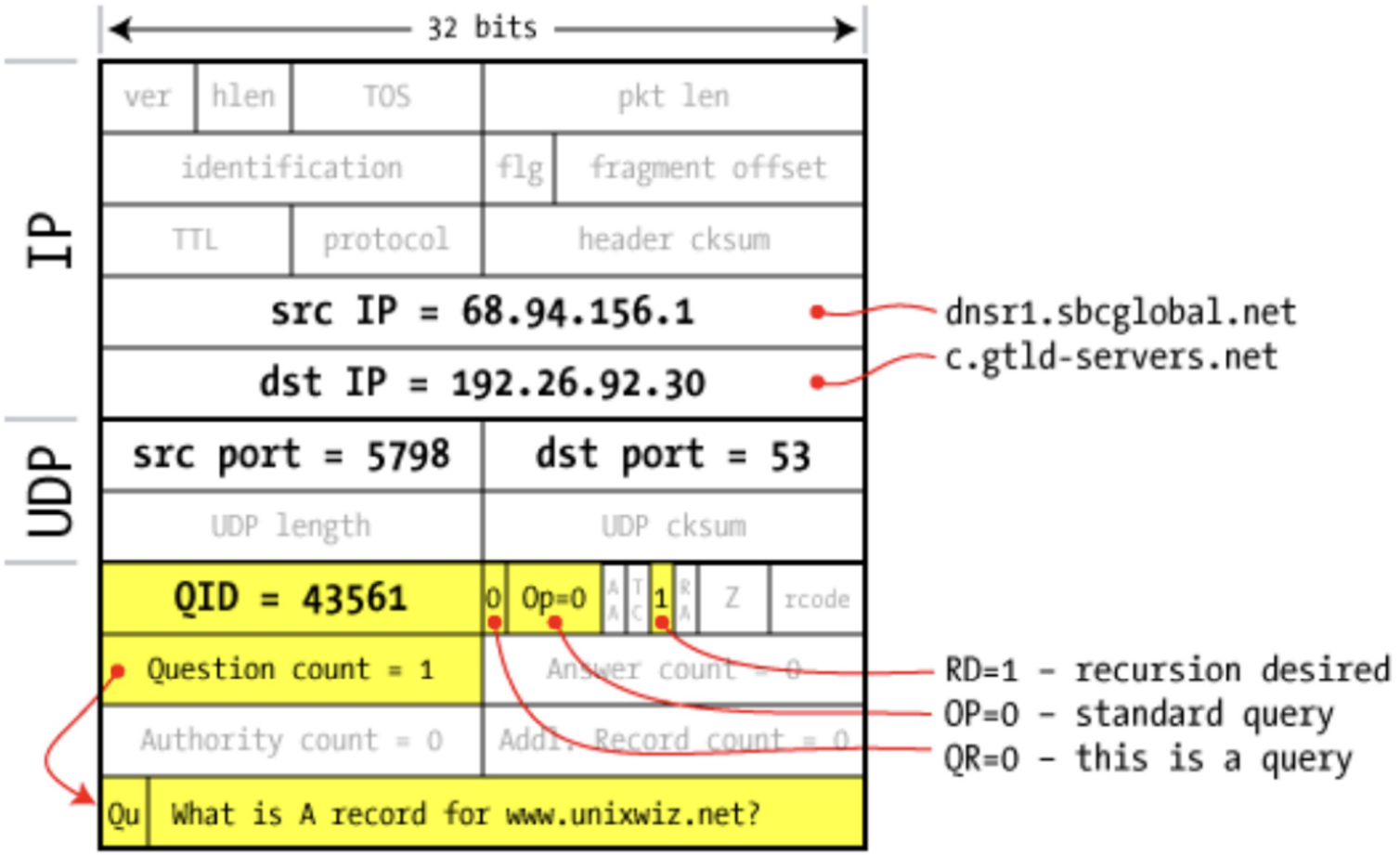


Amplification Attacks

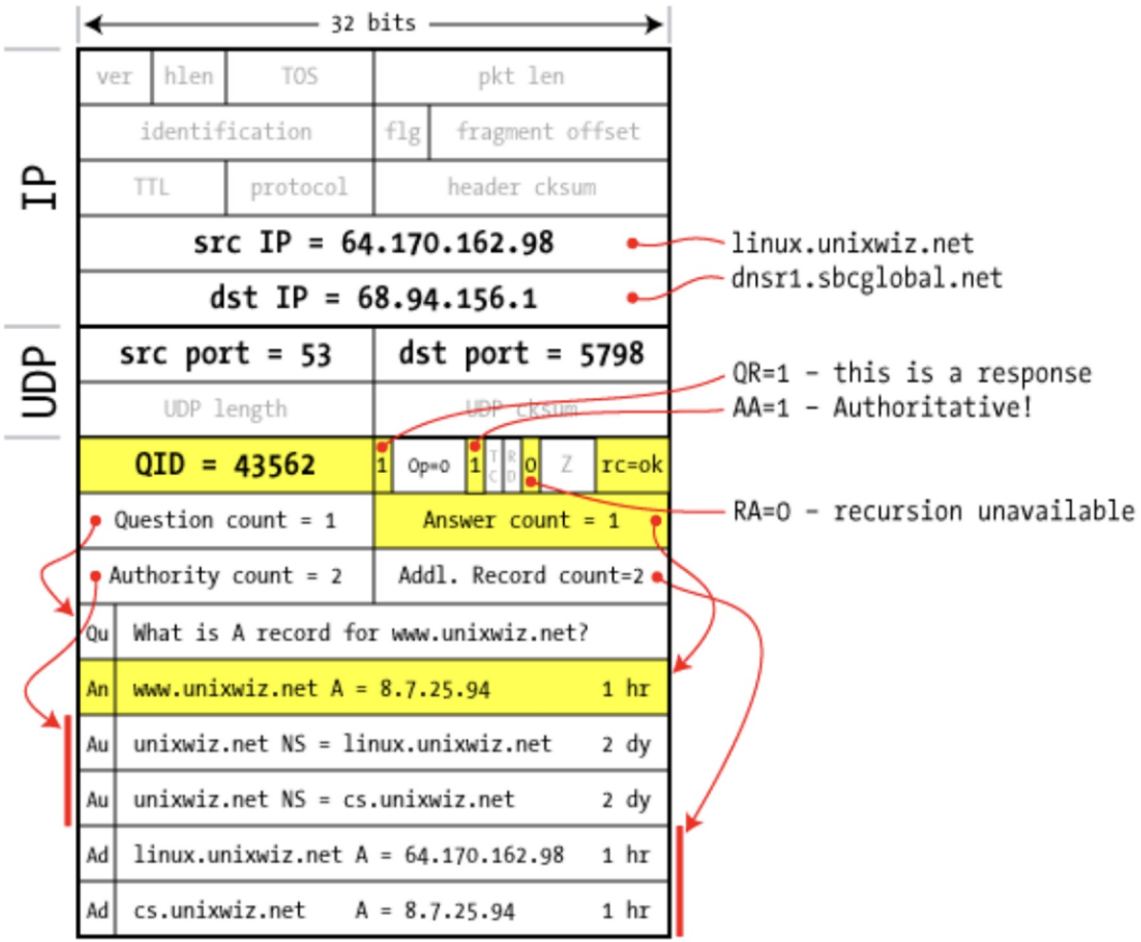
Amplification Attacks are a type of reflection attacks where the victim receives more traffic than the attacker sends.

- Obvious asymmetry
- DNS is a common vector for them
  - Request: 10s of bytes
  - Response: 100s of bytes

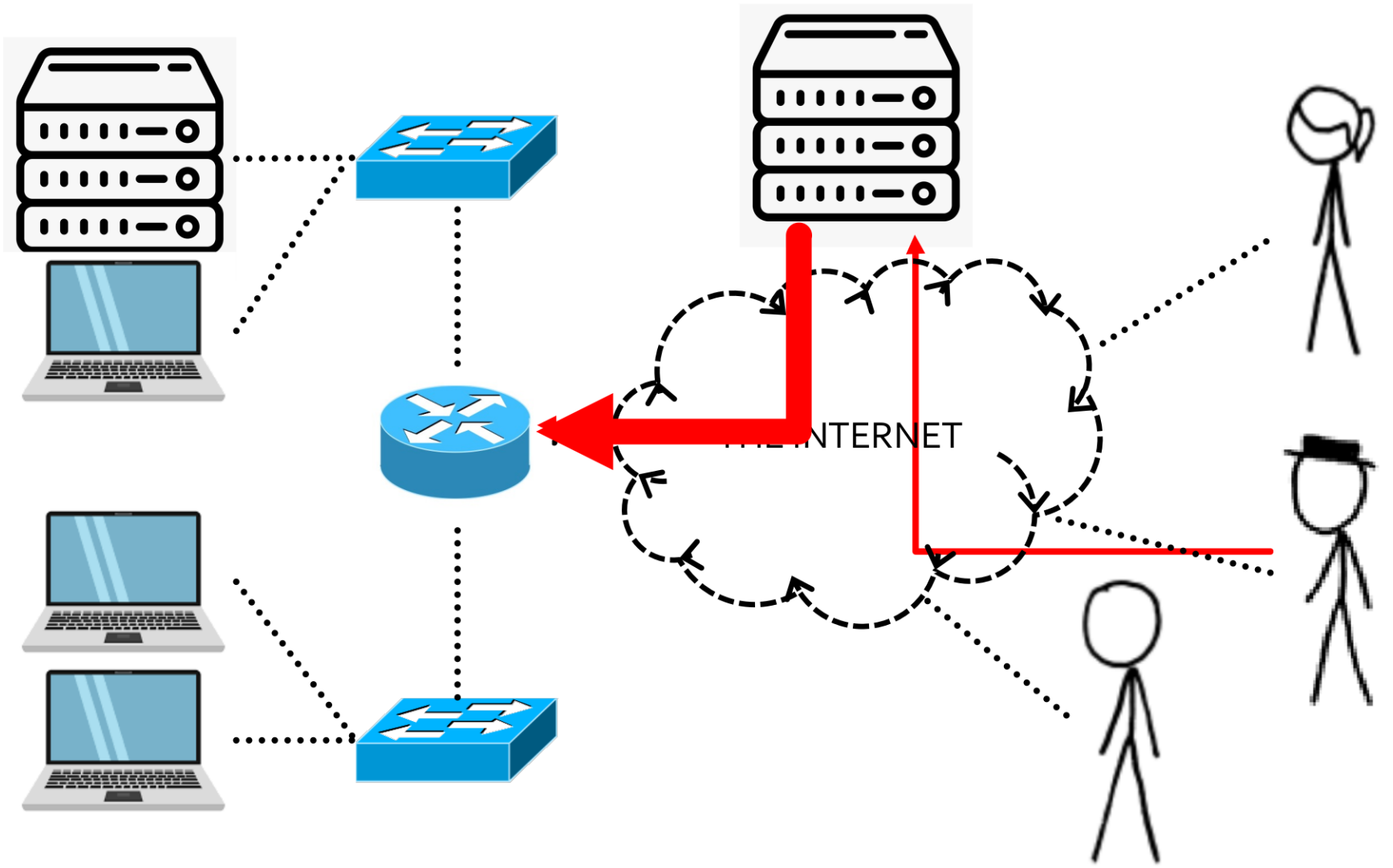
DNS Request


32 bits
IP
UDP
ver
hlen
TOS
pkt len
identification
flg
fragment offset
TTL
protocol
header cksum
src IP = 68.94.156.1
dst IP = 192.26.92.30
src port = 5798
dst port = 53
UDP length
UDP cksum
QID = 43561
0
Op=0
1
Z
rcode
Question count = 1
Authority count = 0
Qu
What is A record for www.unixwiz.net?
dnsr1.sbcglobal.net
c.gtld-servers.net
RD=1 - recursion desired
OP=0 - standard query
QR=0 - this is a query

DNS Response



Amplification Attacks

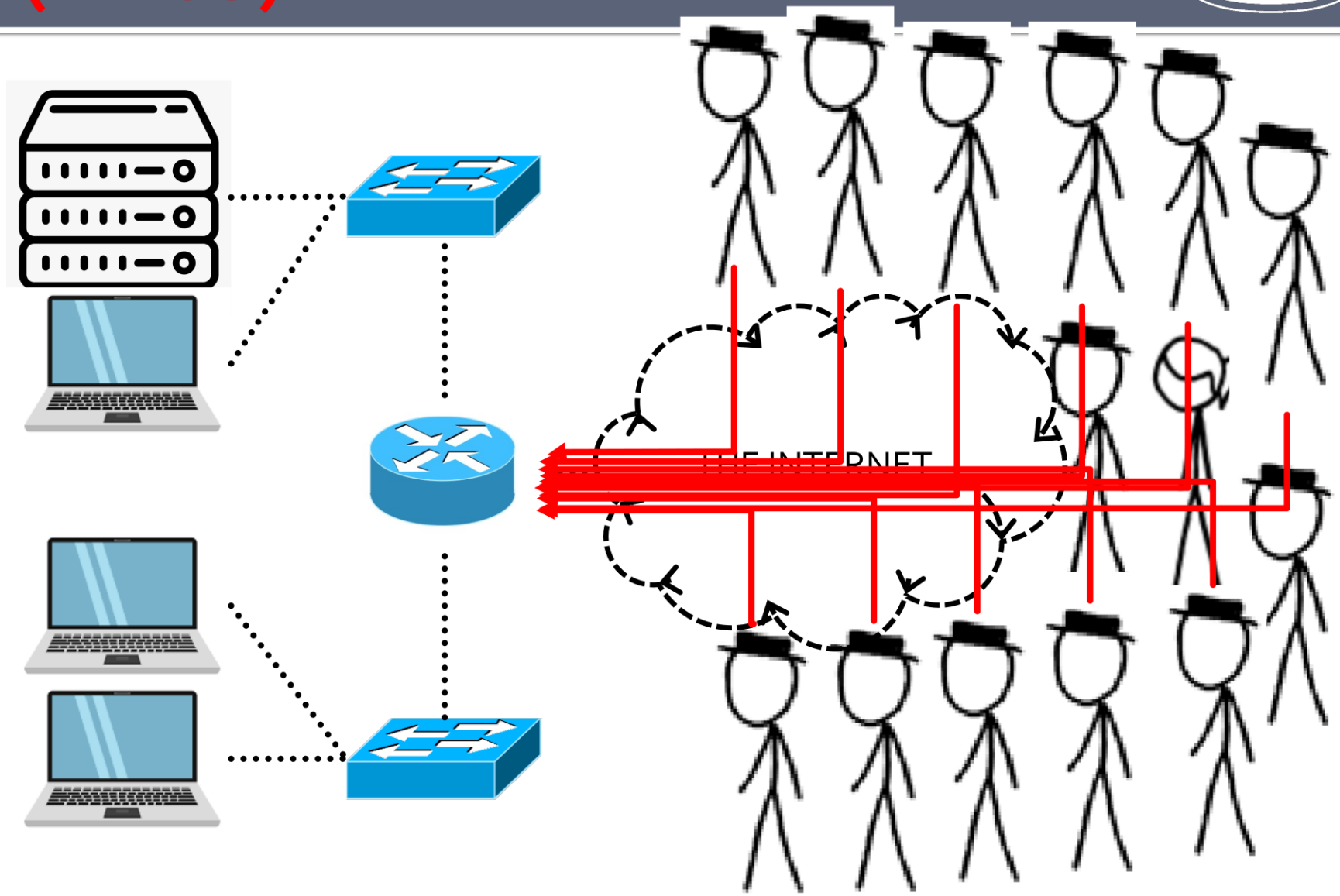


Distributed Denial of Service (DDoS)

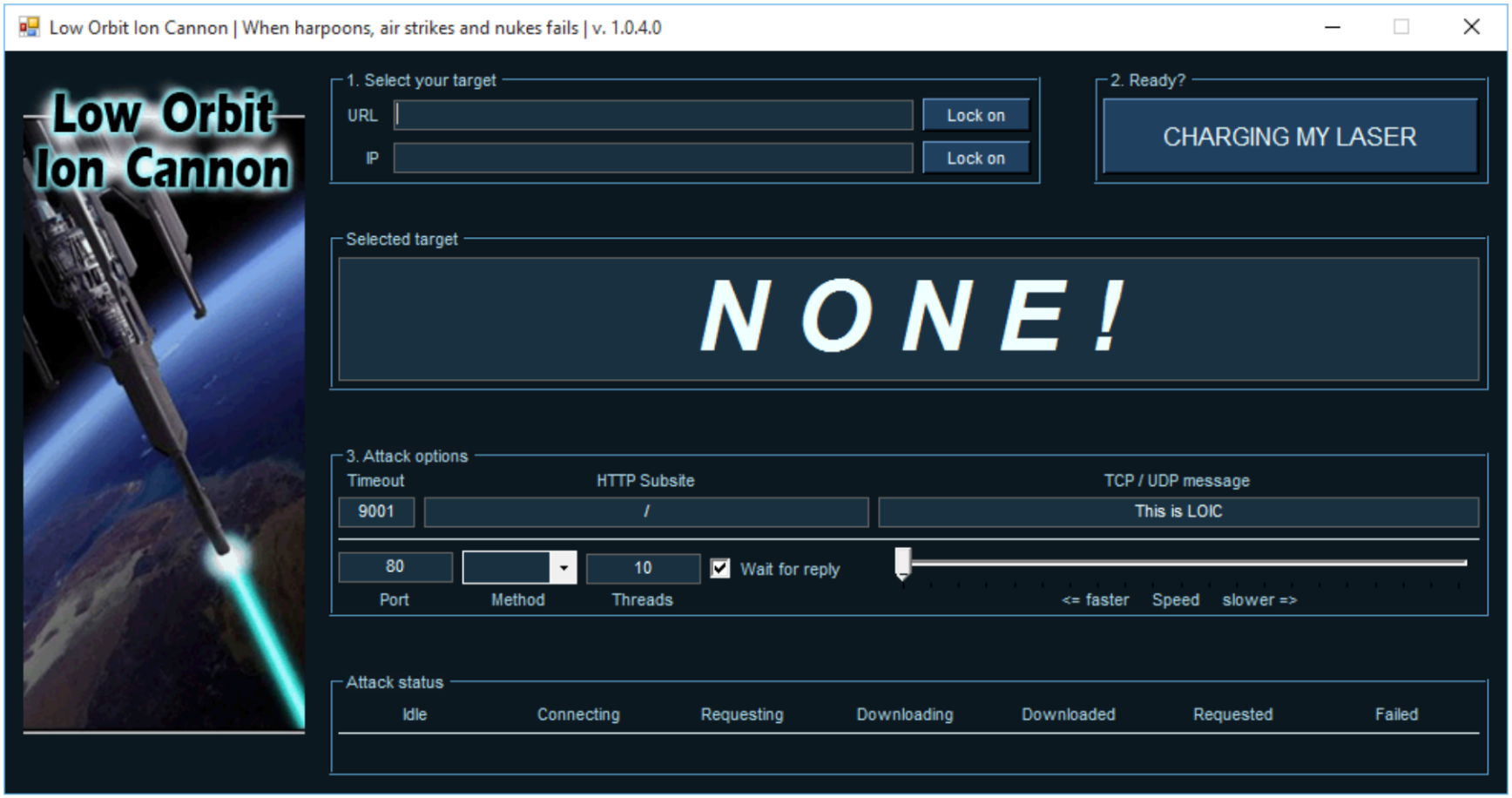
Distributed Denial of Service (DDoS) is a type of DoS attack where the "source" of the attack is distributed across the Internet.

- Often accomplished via botnets
- Each bot under the attacker's control contributes negligible amount of traffic but the sum is non-negligible

Distributed Denial of Service (DDoS)

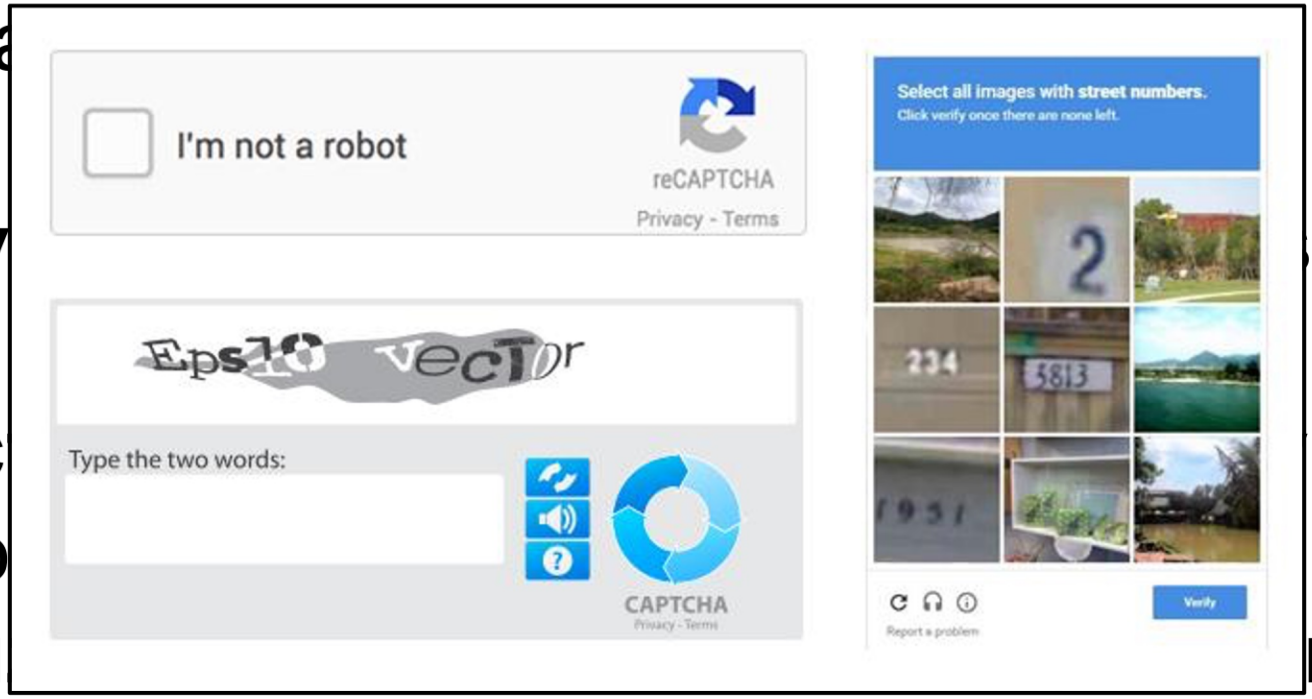


Script-Kiddie Tools



DoS Defenses

Basic DoS defenses are relatively straight-forwa

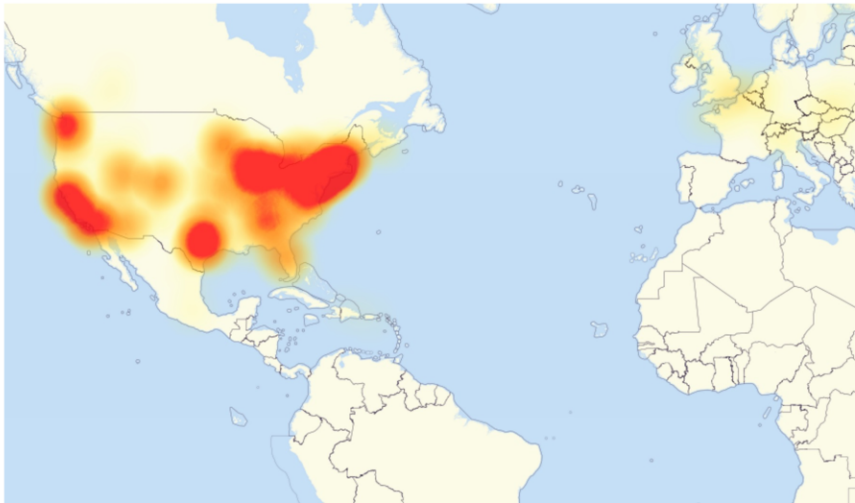


- **Ov** built for
- **Ac** blo
- **Pu** r requires client to solve CAPTCHA

Massively, Massive Botnets

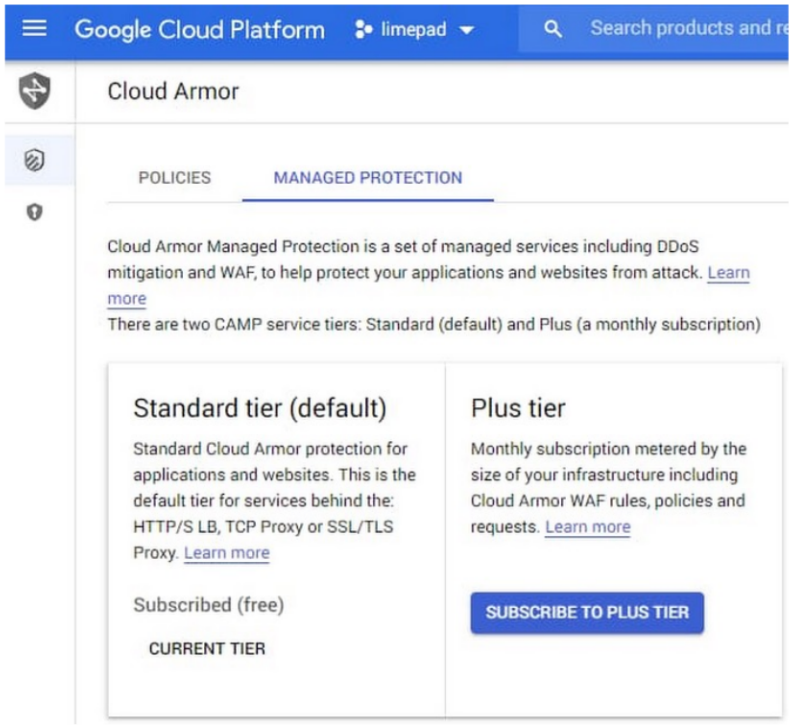
The **Mirai Botnet** was mostly comprised of IoT/embedded devices breached via default usernames/passwords.

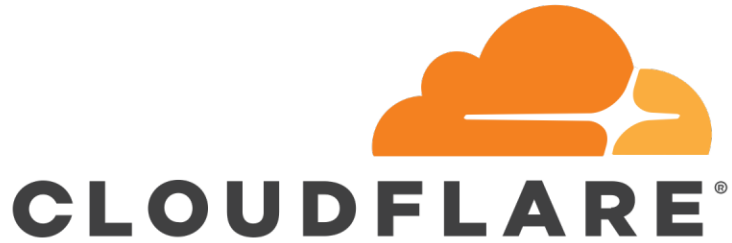
- ~600k bots generating 600GB – 1TB of flood traffic towards victim
- Took down DynDNS for ~2 hours in 2016
  - Major provider for US



DoS Defenses

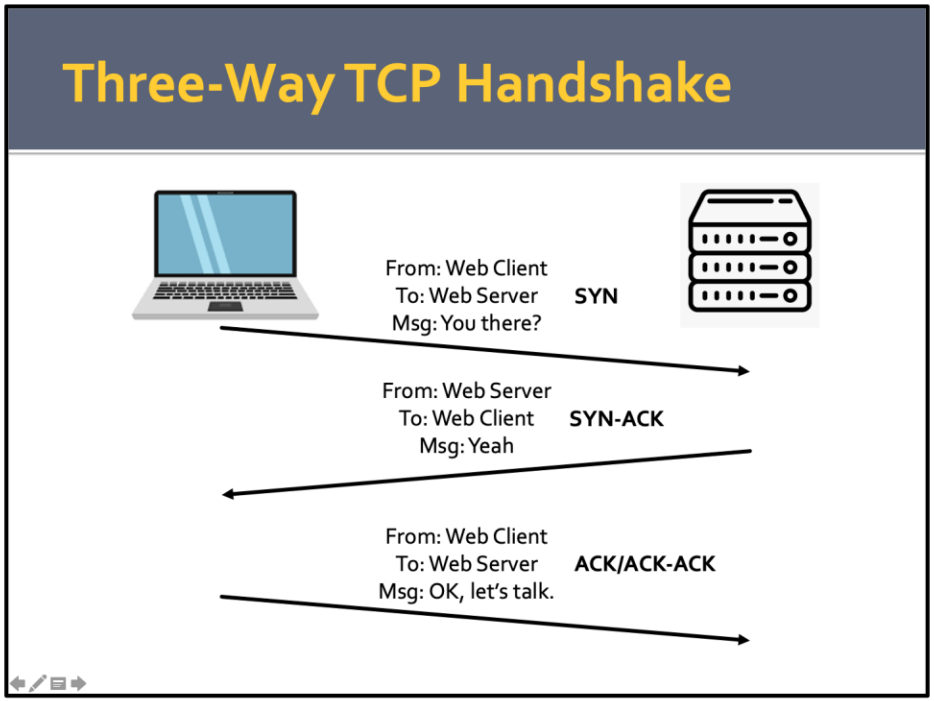
Advanced DoS attacks require specialized defenses and custom infrastructure.



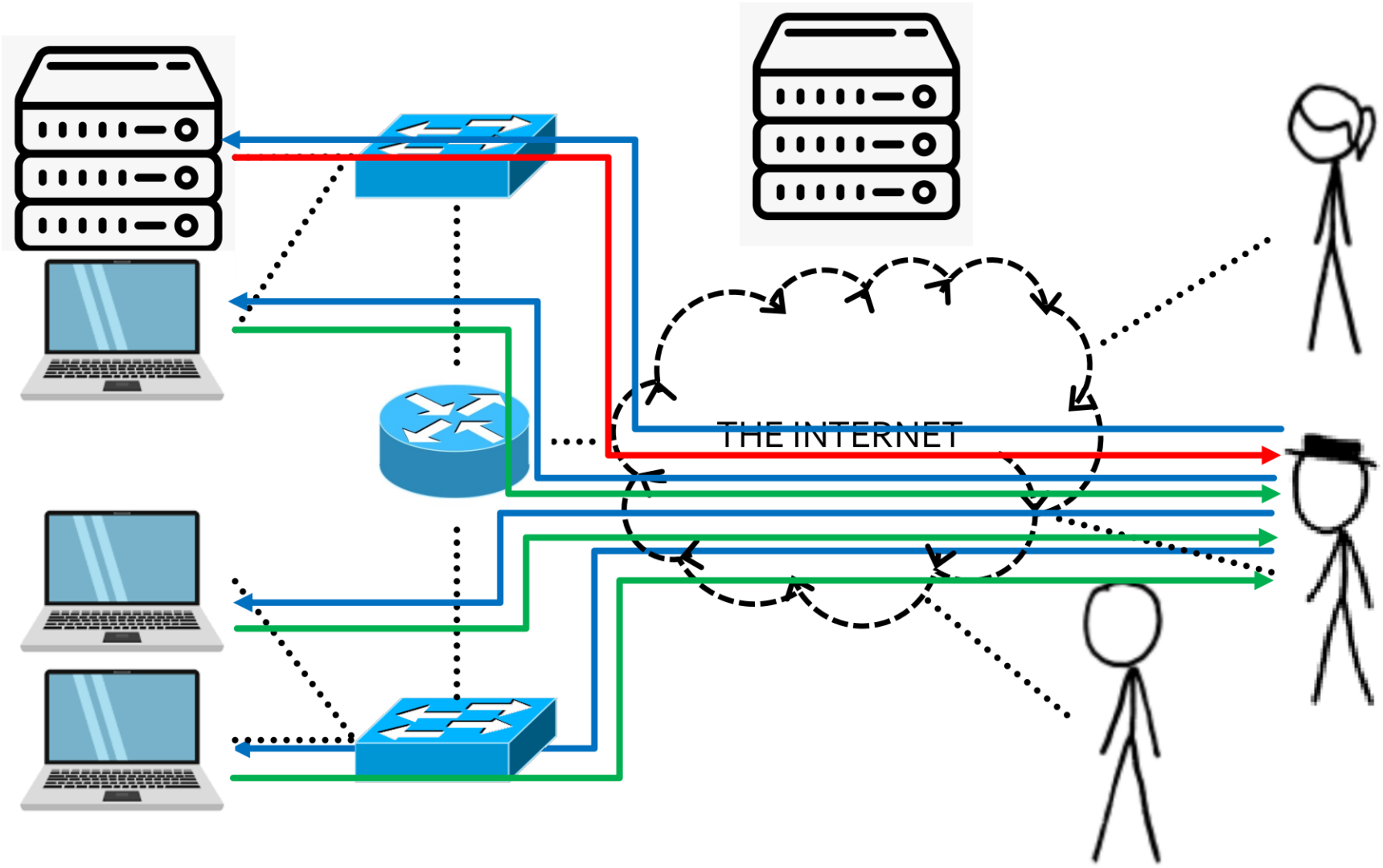


Port Scanning

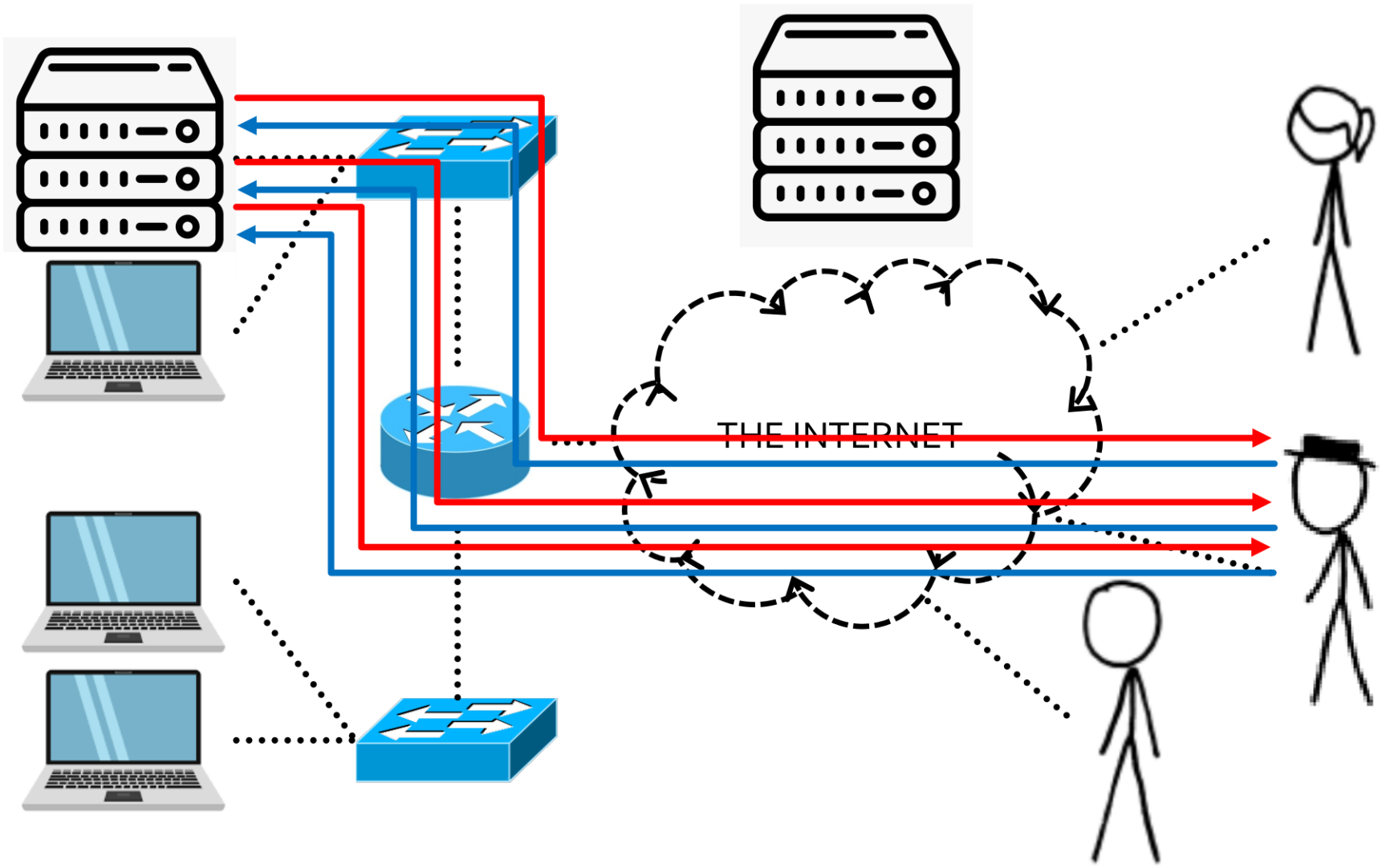
Port scanning is a reconnaissance technique that is used by attackers to gain information to aid them in their attacks.



Horizontal Port Scanning



Vertical Port Scan



Computer and Network Security

Lecture 17: WWW/Web-Attacks

COMP-5370/6370
Fall 2025