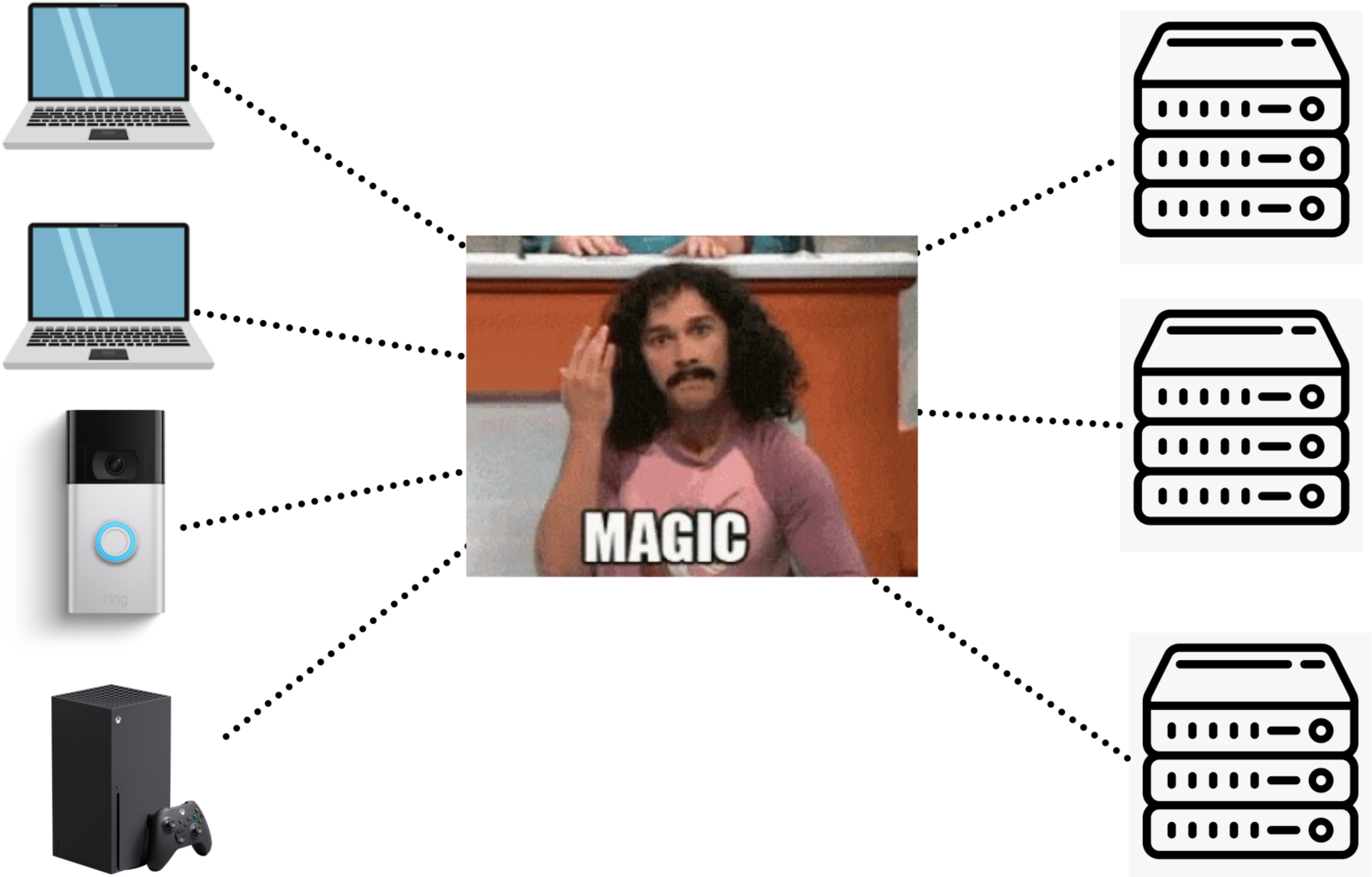
AI for Security (AI4Sec)

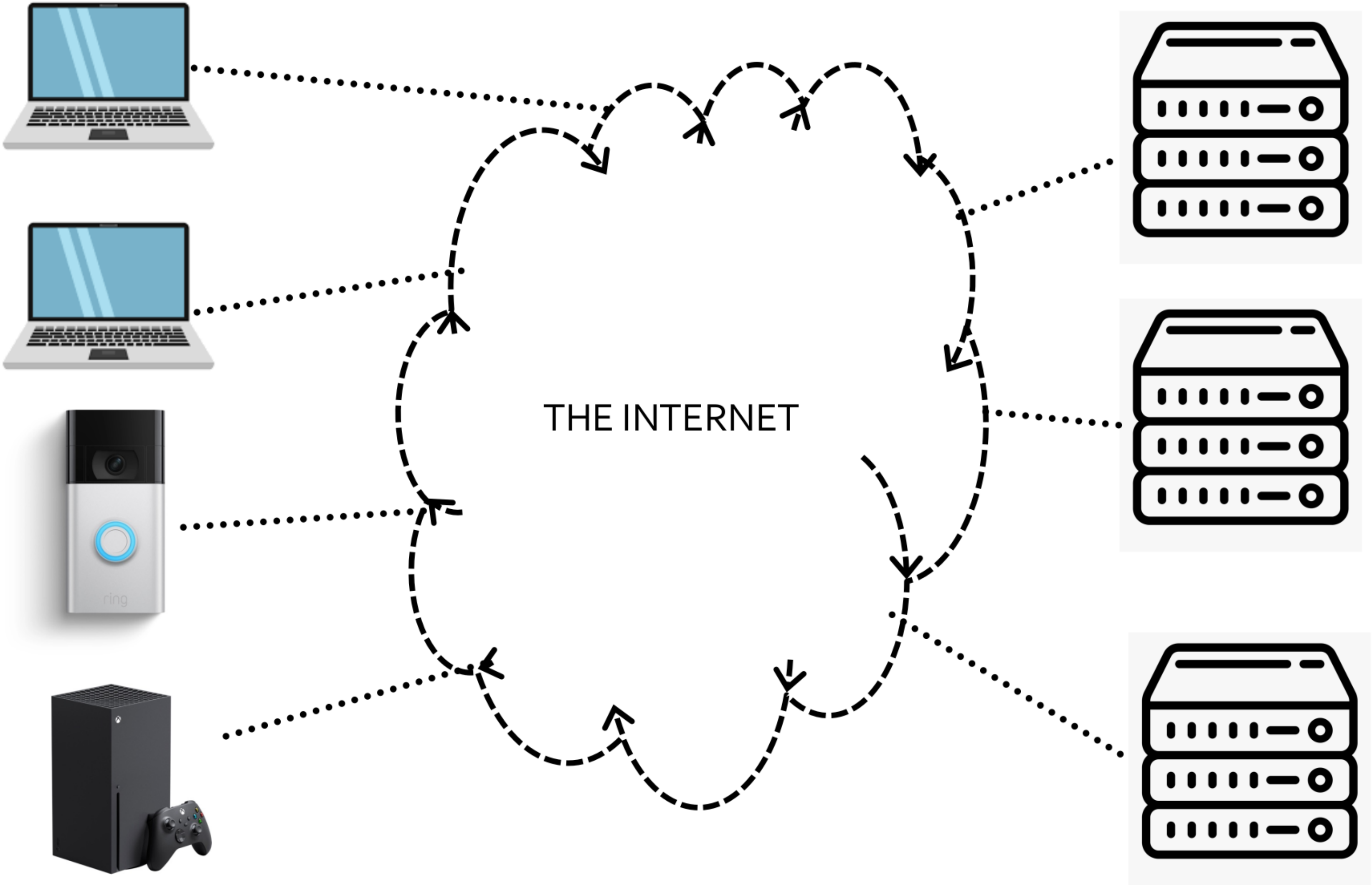
Network Security Overview

COMP-5870/6870

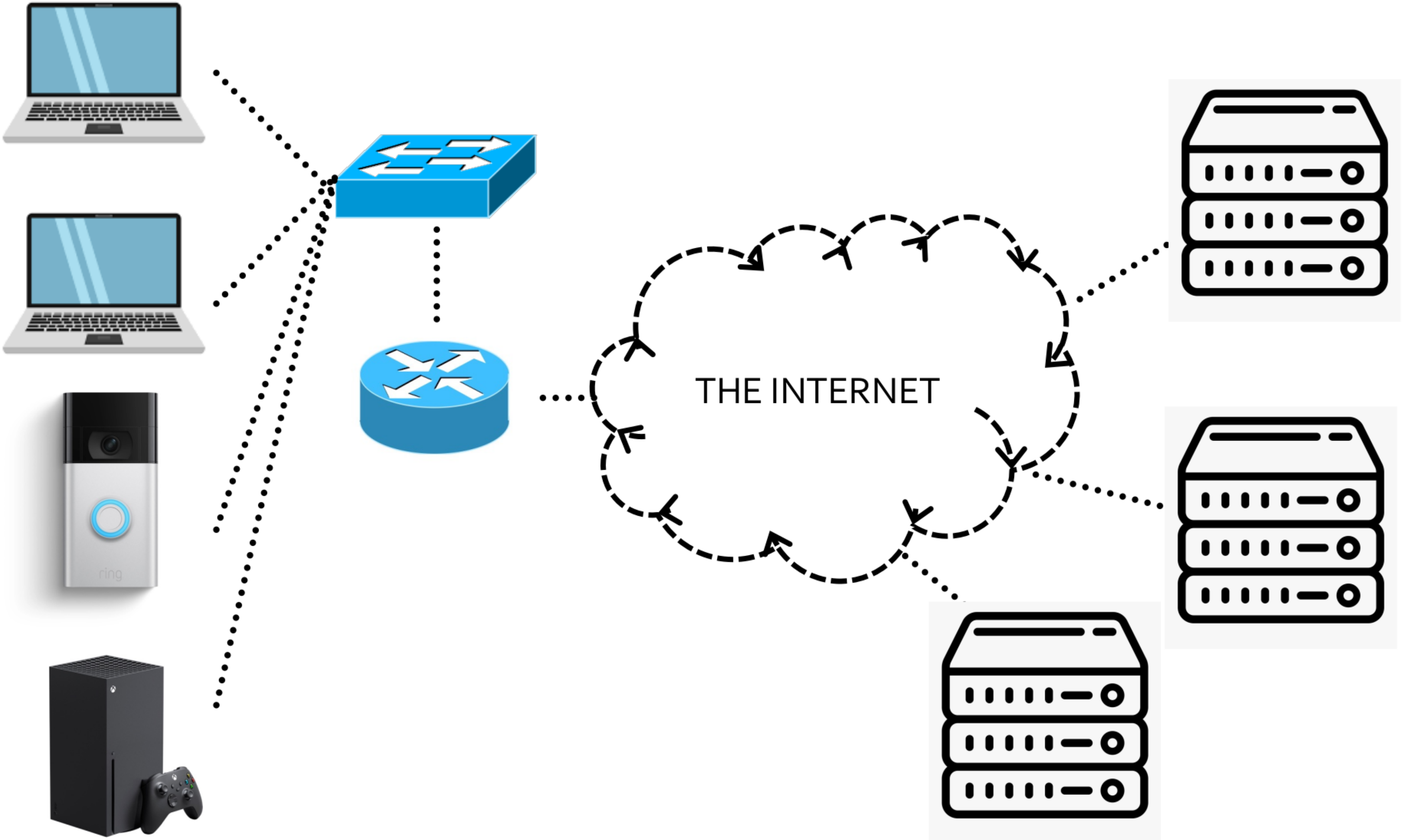
ring

ring


MAGIC
ring

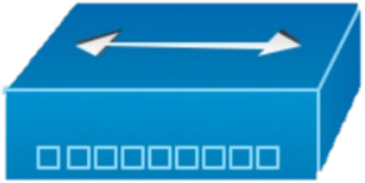

THE INTERNET

Home Network



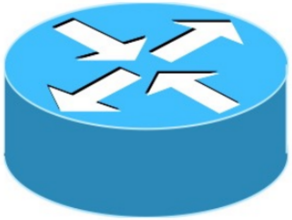
Network Devices

- **Hubs** are L1 devices
  - Packet comes in, packets go-out

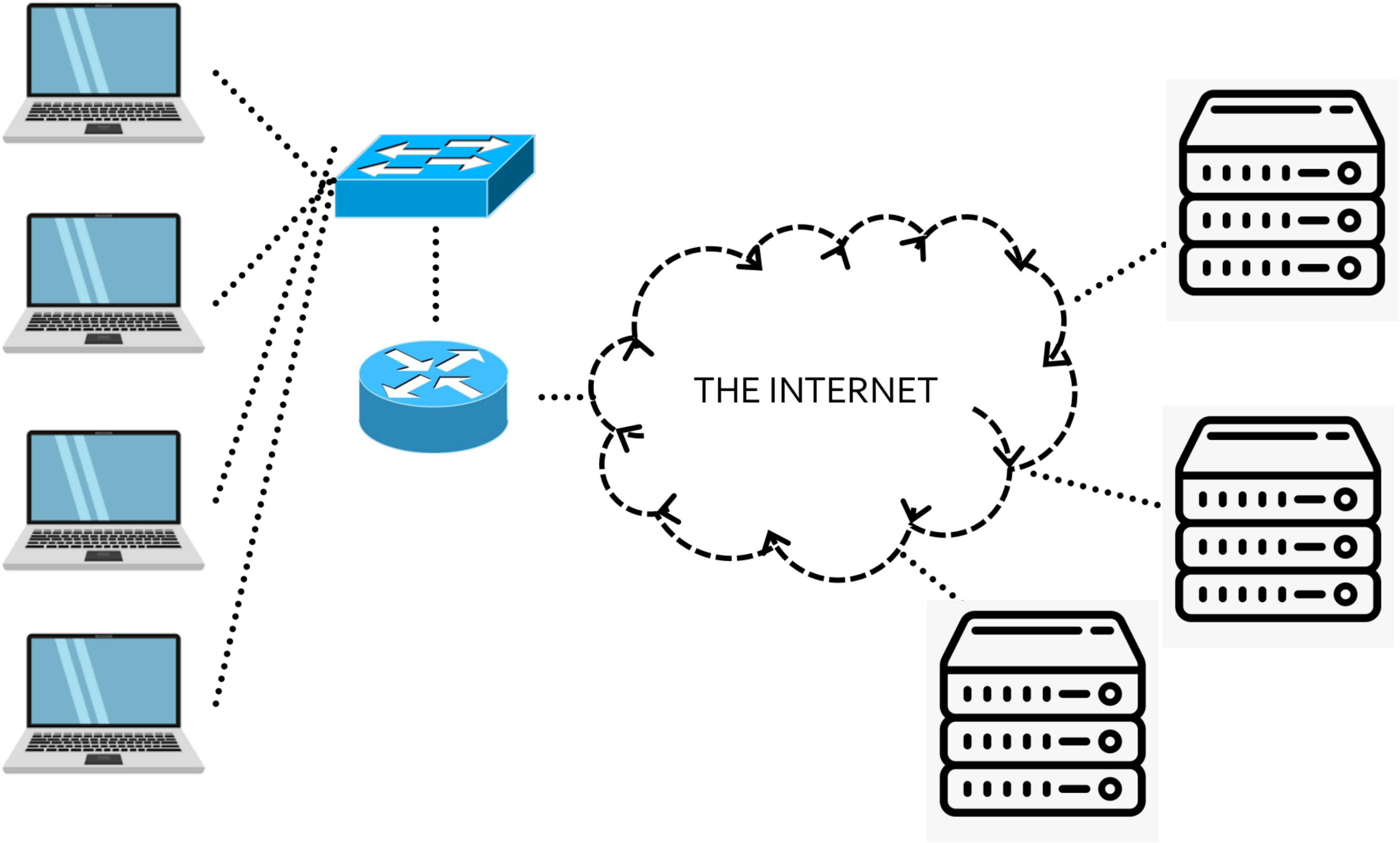


- **Switches** are L2 devices
  - Dispatch packets via MAC address
  - “L3 switches” are common but are not what we’re talking about

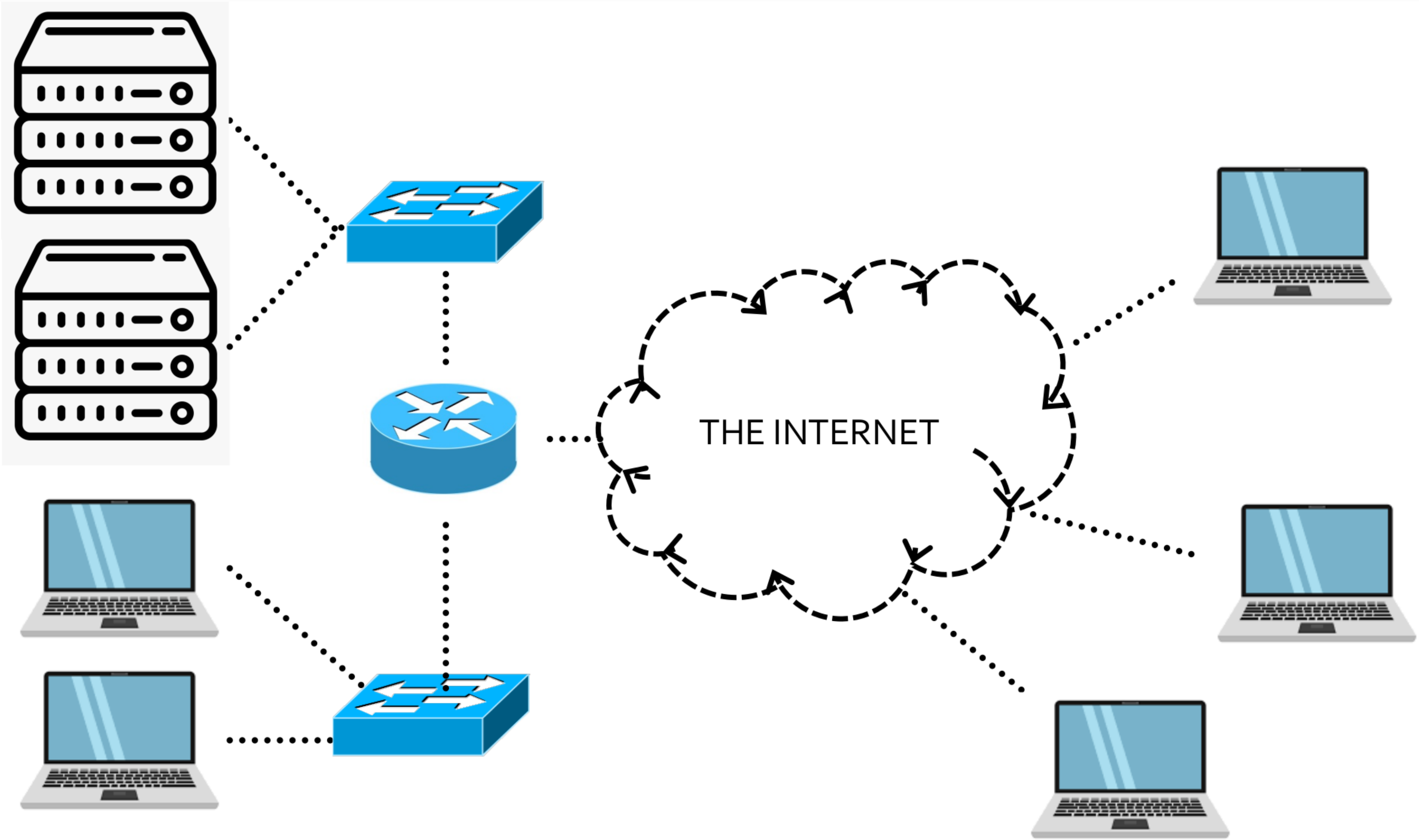
- **Routers** are L3 devices
  - Dispatch packets via IP address
  - Lots of things called “routers” aren’t actually **routers** (but some are)



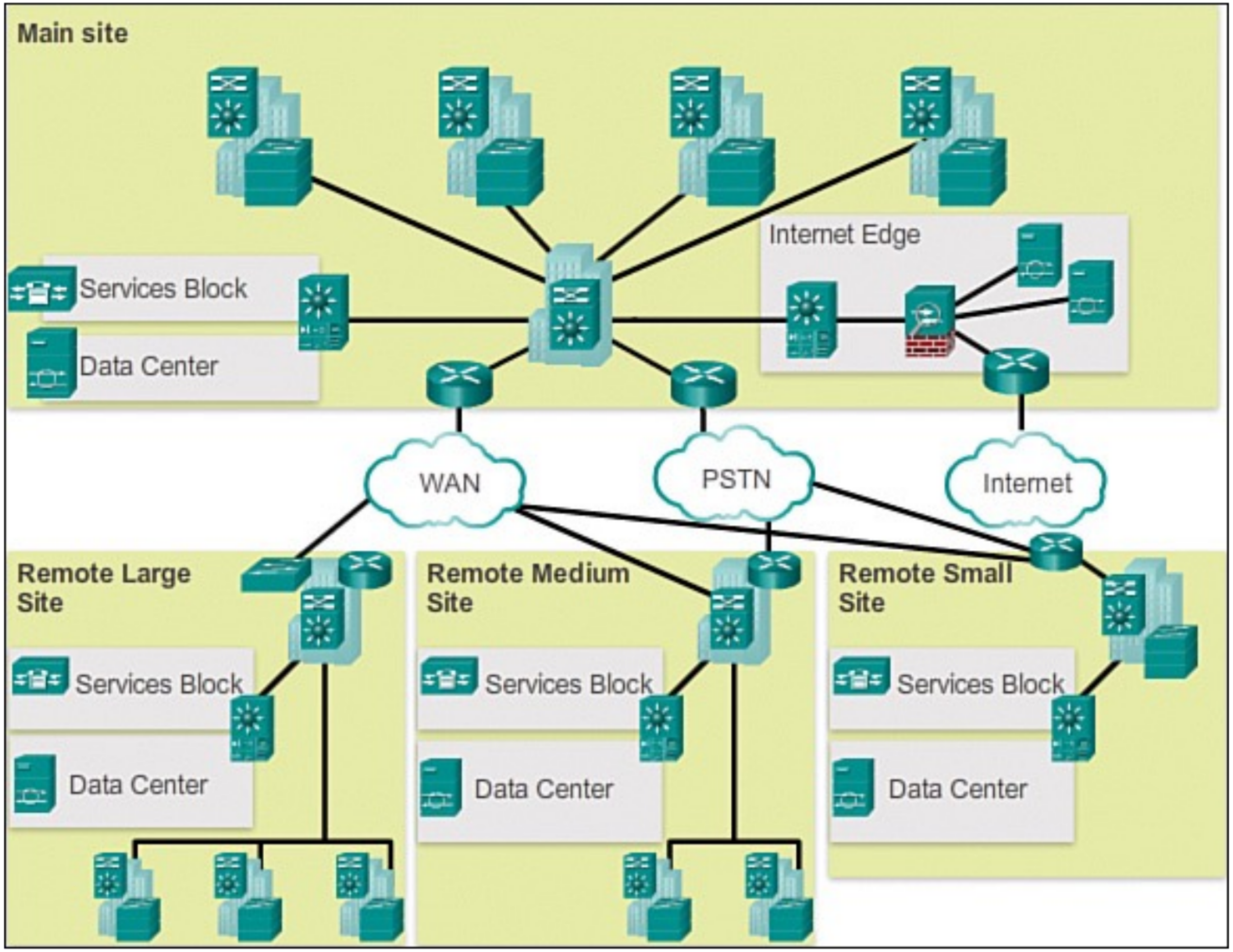
Home Network



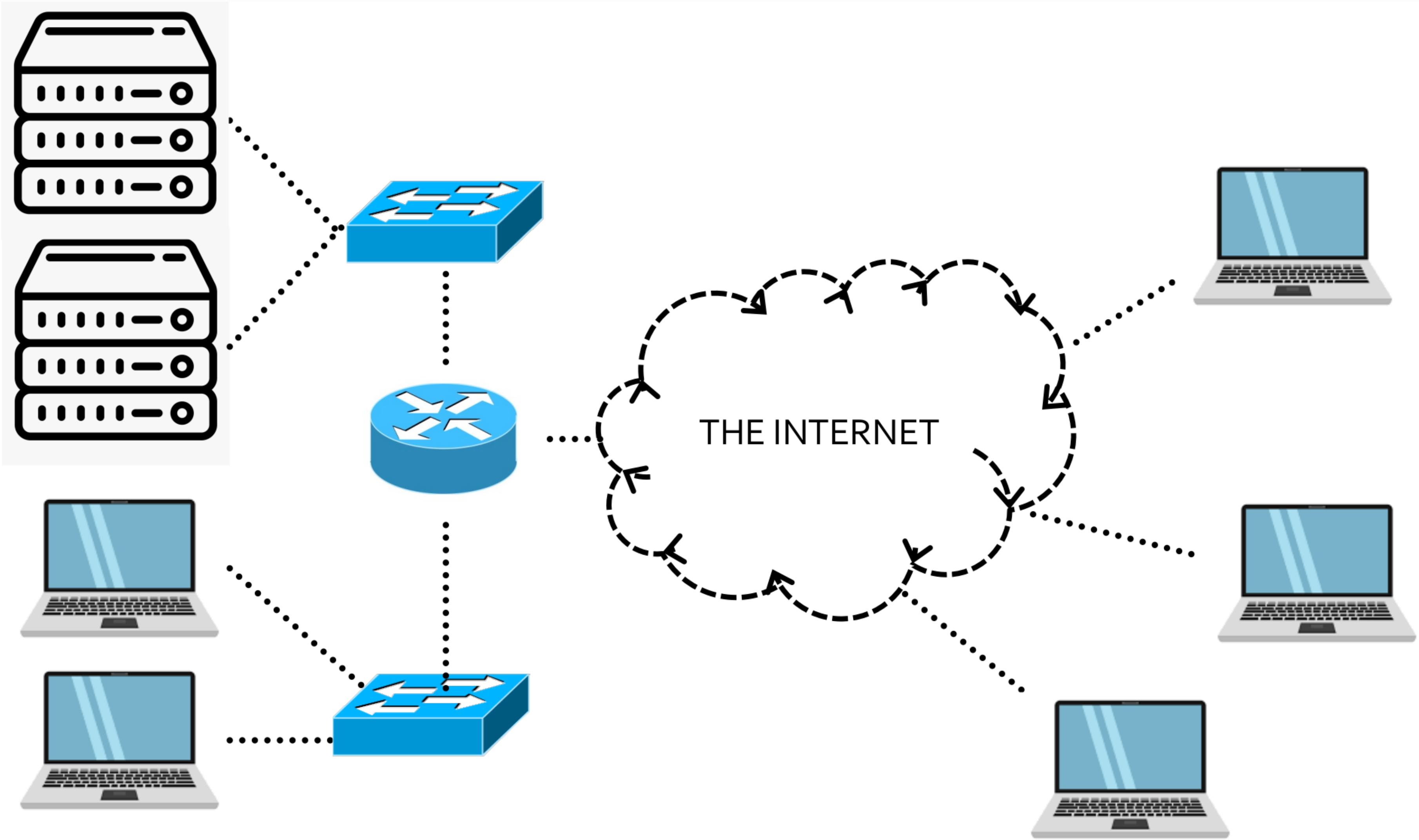
Simple Enterprise Network



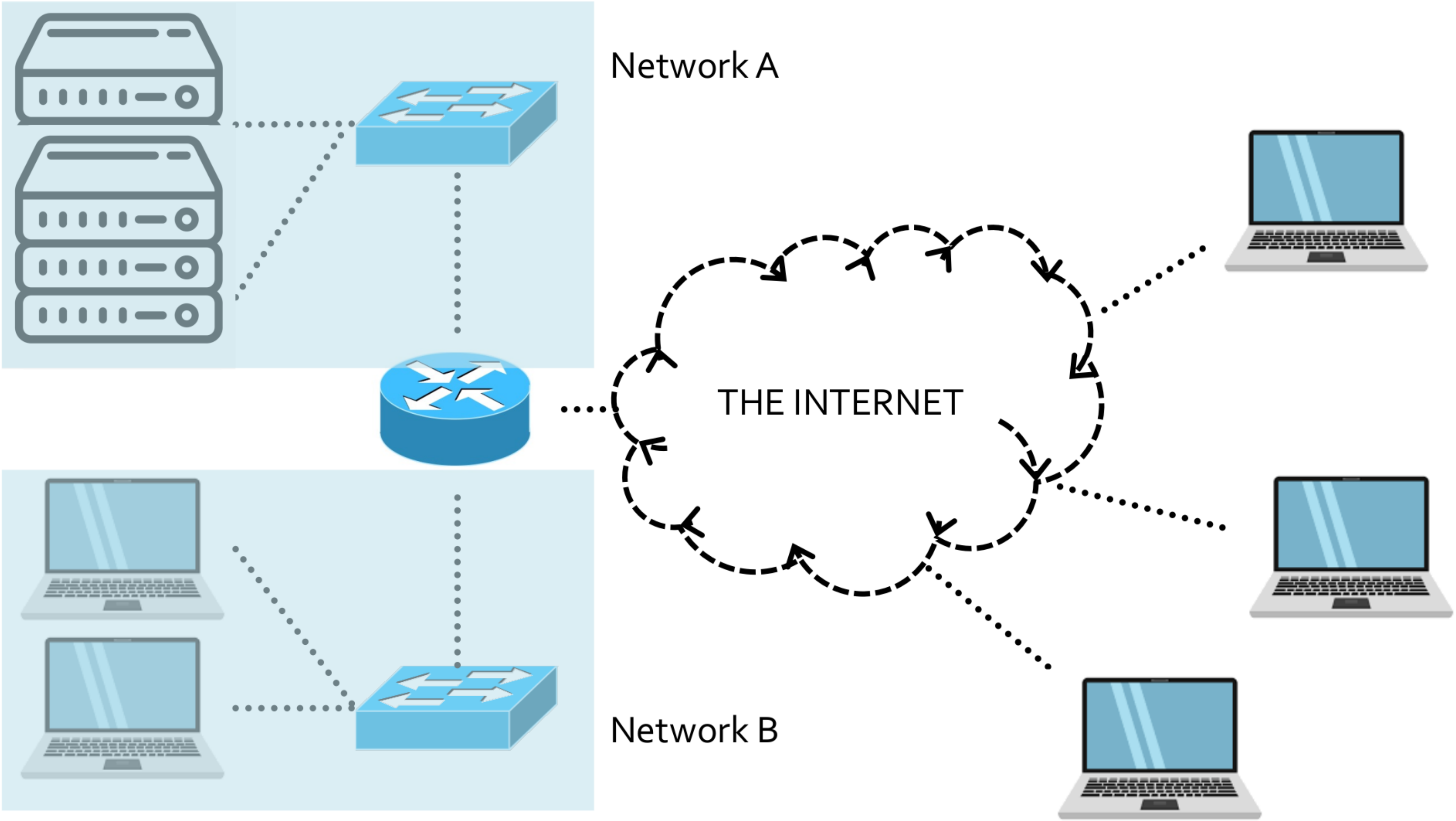
Enterprise Network

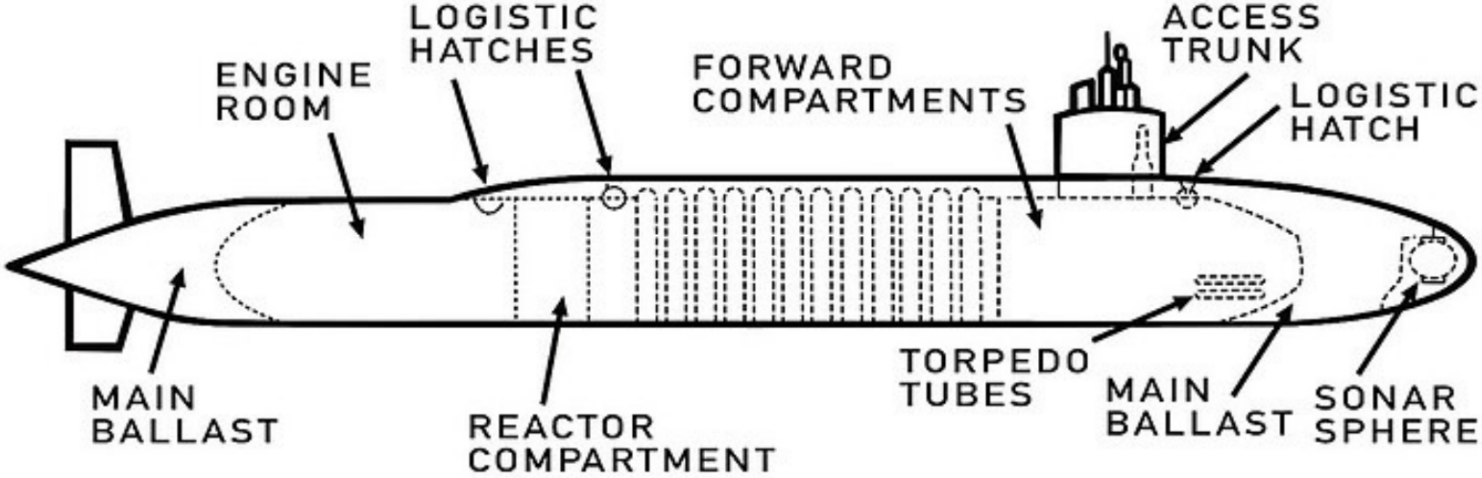


Simple Enterprise Network



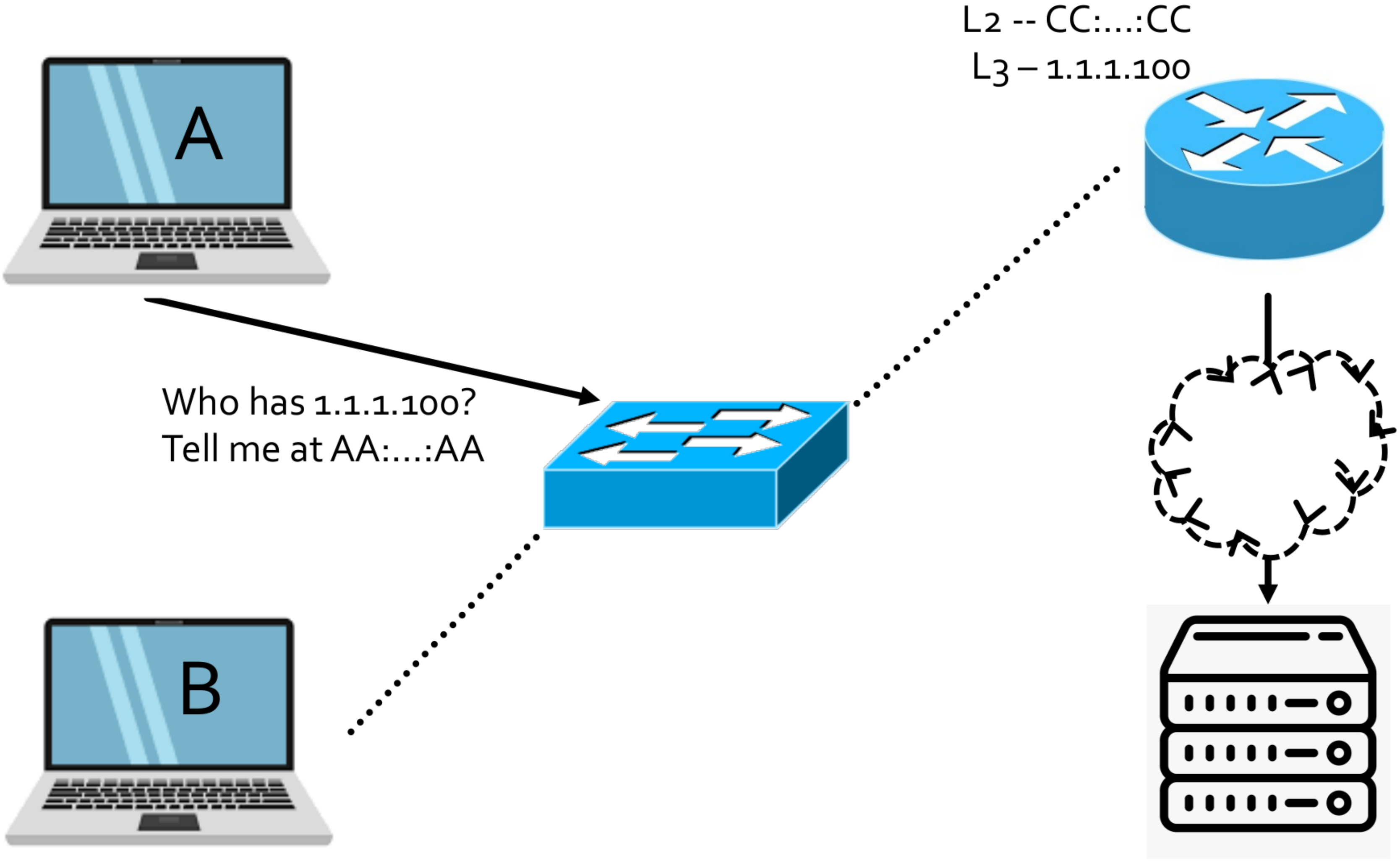
Network Segmentation



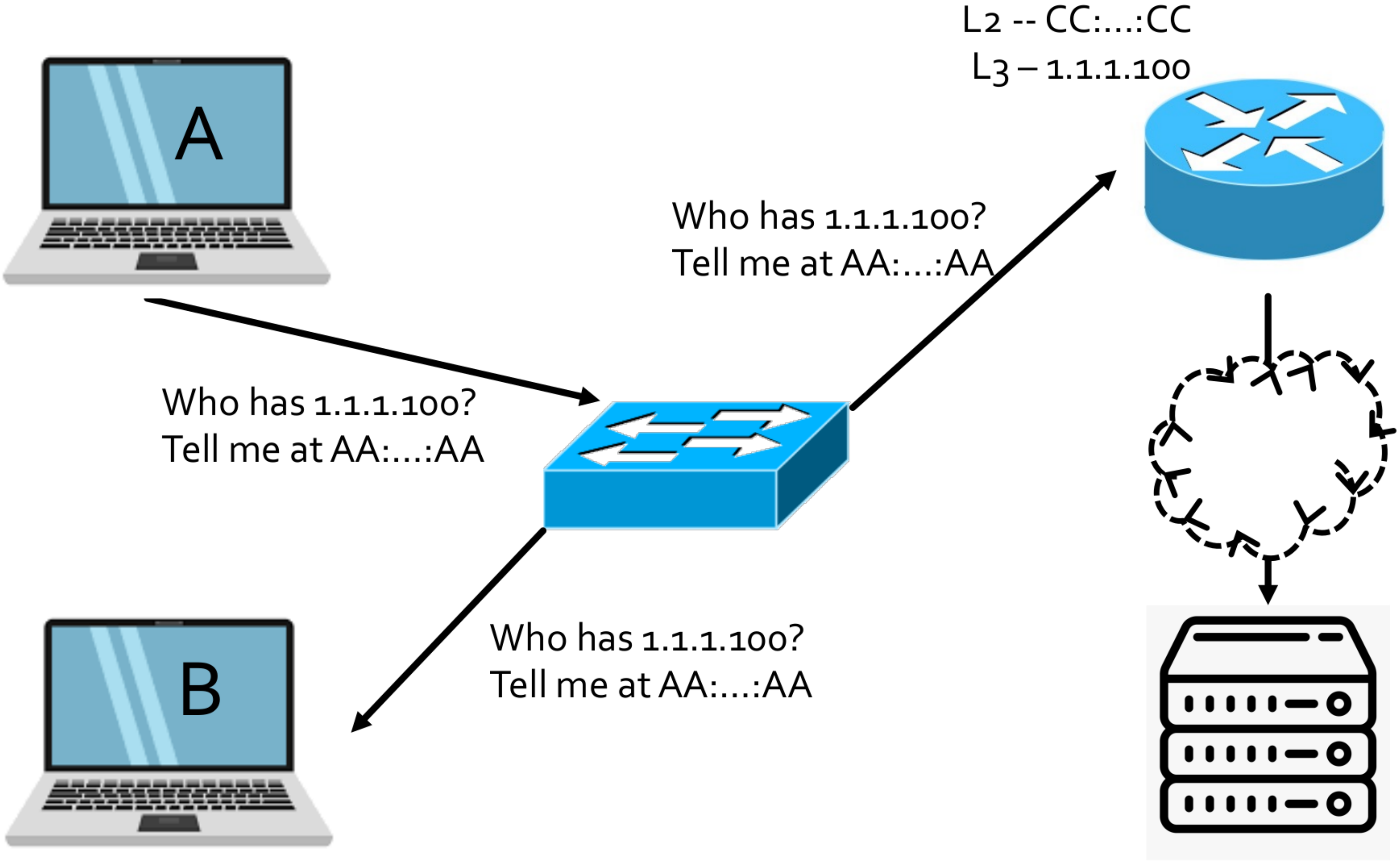


OHIO-CLASS SUBMARINE

Network Broadcasts (ARP)



Network Broadcasts (ARP)



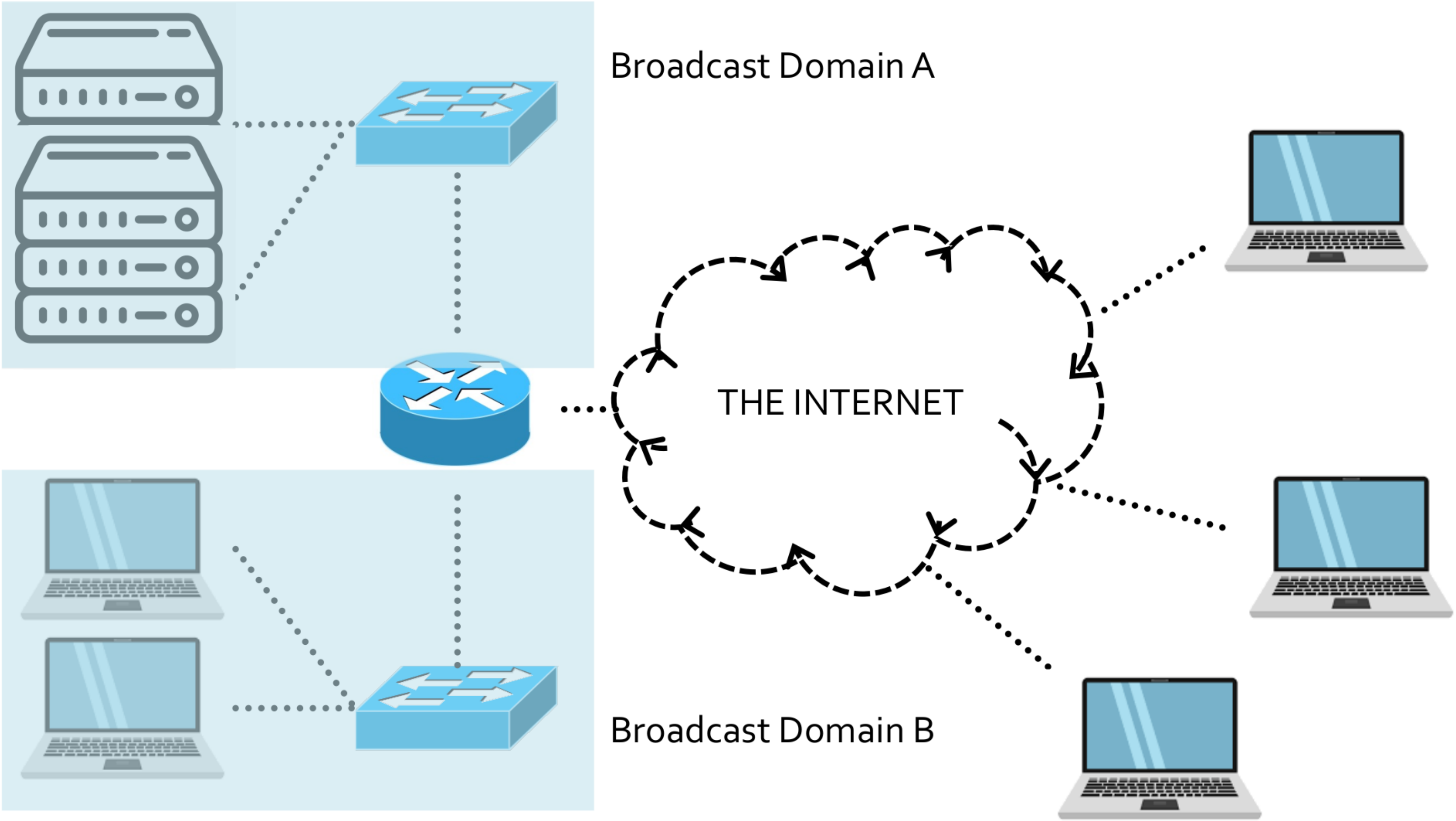
L2 -- CC:...:CC
L3 – 1.1.1.100

Who has 1.1.1.100?
Tell me at AA:...:AA

Who has 1.1.1.100?
Tell me at AA:...:AA

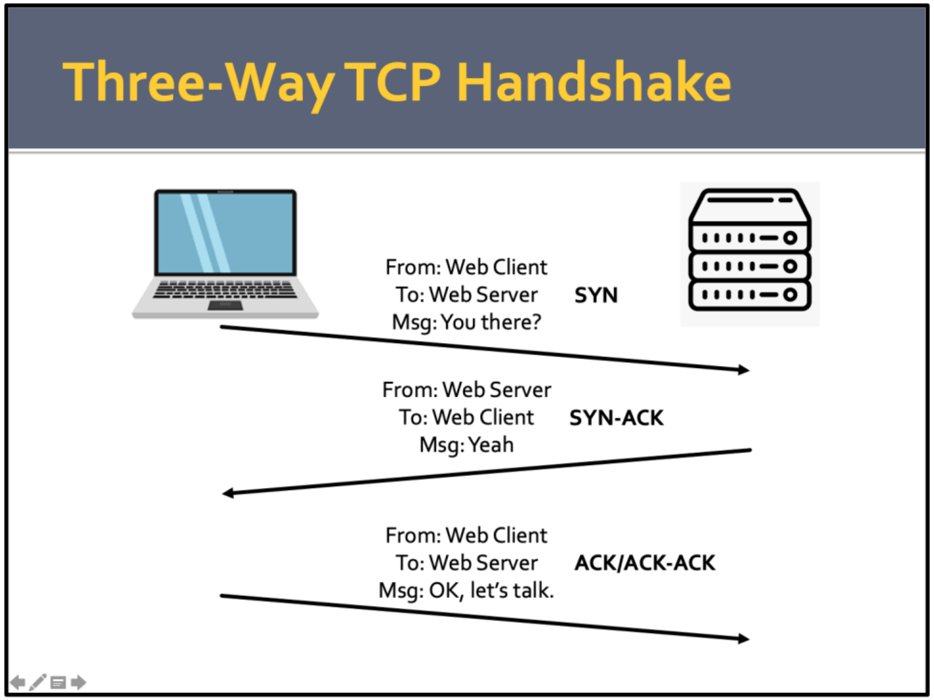
Who has 1.1.1.100?
Tell me at AA:...:AA

Broadcast Domains



Port Scanning

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



Three-Way TCP Handshake

From: Web Client
To: Web Server
Msg: You there?

SYN

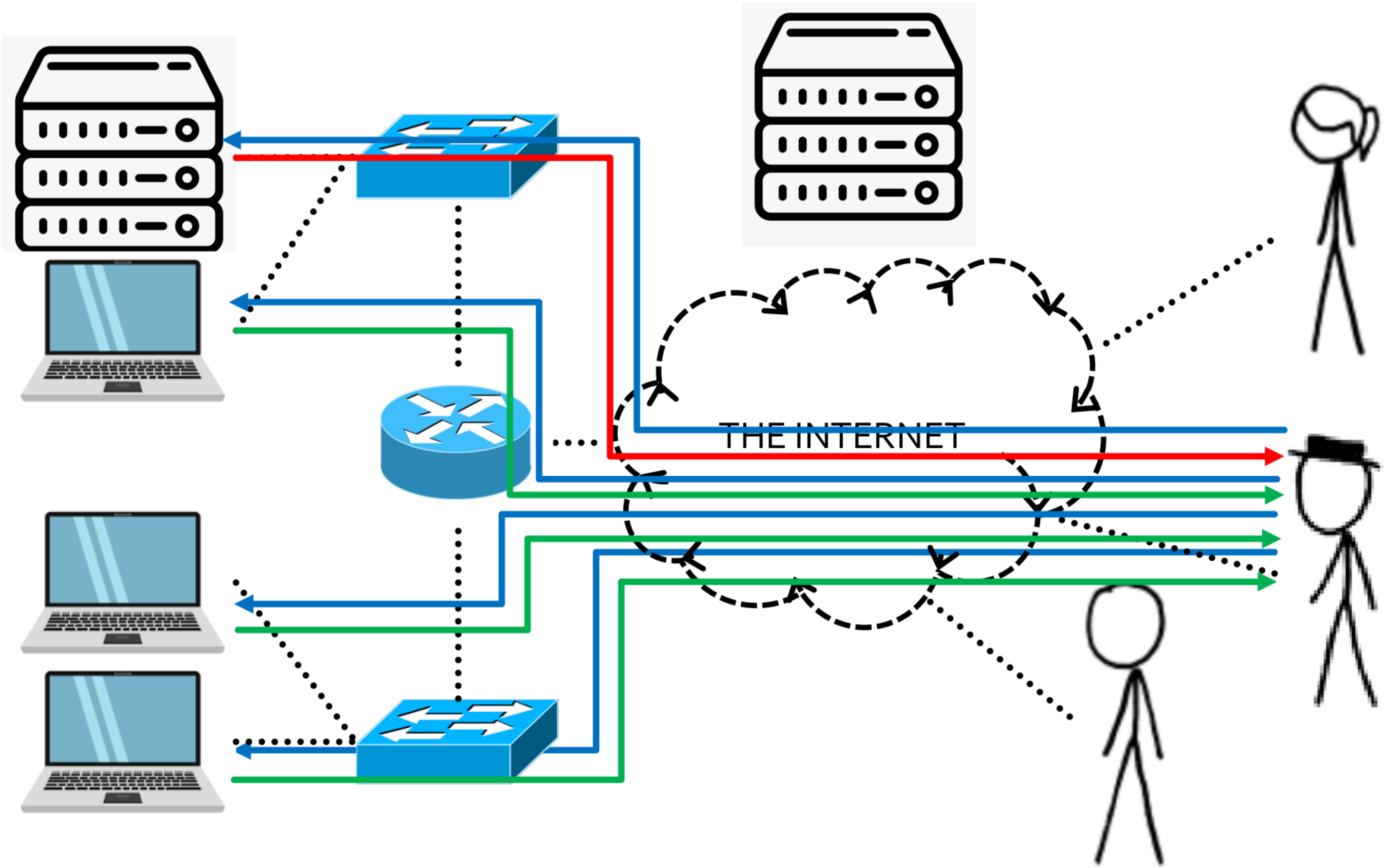
From: Web Server
To: Web Client
Msg: Yeah

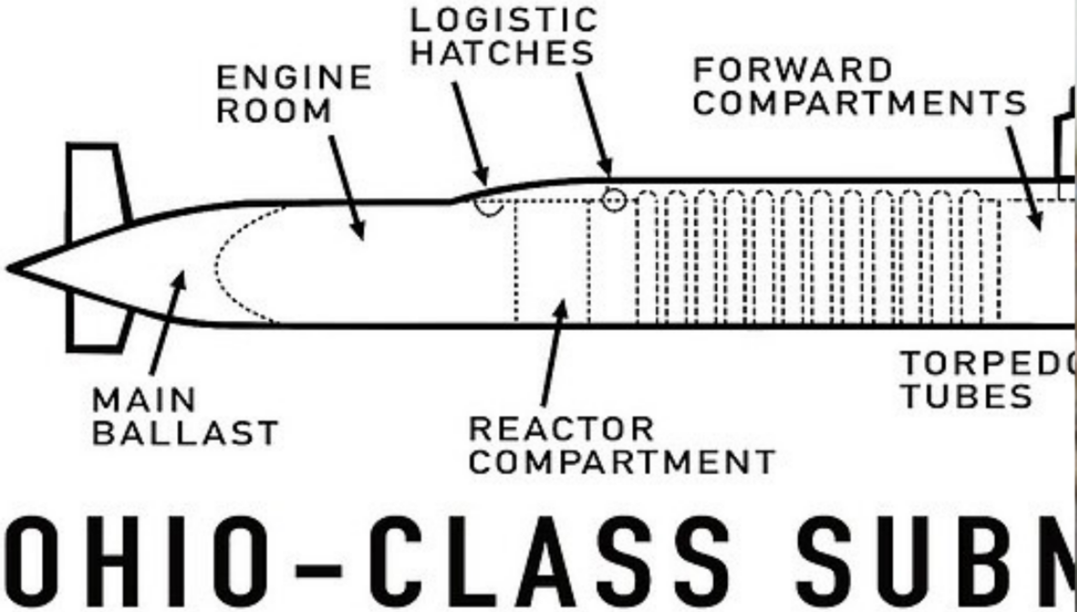
SYN-ACK

From: Web Client
To: Web Server
Msg: OK, let's talk.

ACK/ACK-ACK

Port Scanning




LOGISTIC HATCHES
ENGINE ROOM
FORWARD COMPARTMENTS
MAIN BALLAST
REACTOR COMPARTMENT
TORPEDO
TUBES
OHIO-CLASS SUBN

Firewalls

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

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)

Canonical Protocols

Application Layer Protocol	Transport Layer Protocol	Port	Name
FTP	TCP	20	File Transfer Protocol – Data
FTP	TCP	21	FTP – Connection
Telnet	TCP	23	Telnet
SMTP	TCP	25	Simple Mail Transfer Protocol
DNS	TCP / UDP	53	Domain Name System – Zone Transfer / Lookups
DHCP	UDP	67 / 68	Dynamic Host Configuration Protocol – Server / Client
HTTP	TCP	80	Hypertext Transfer Protocol
POP3	TCP	110	Post Office Protocol
SNMP	UDP	161	Simple Network Management Protocol (v1,2)
RDP	TCP / UDP	3389	Remote Desktop Protocol

…and many, many more…

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*>

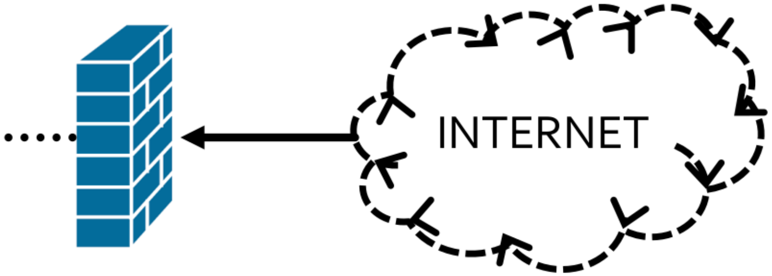
Firewall Implementations

- Blacklisting traffic
  - Match rule? **BLOCK**
- Whitelisting traffic
  - Match rule? **ALLOW**

There’s always a default action if doesn’t match a specific rule!

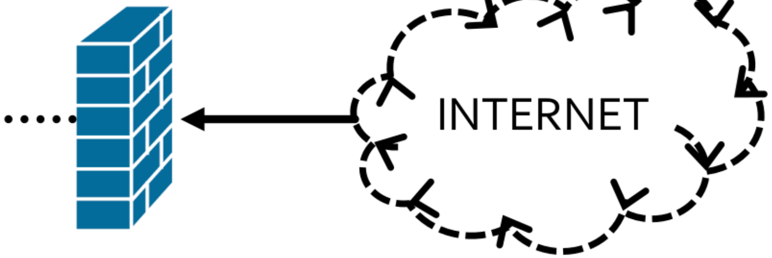
Firewall Example

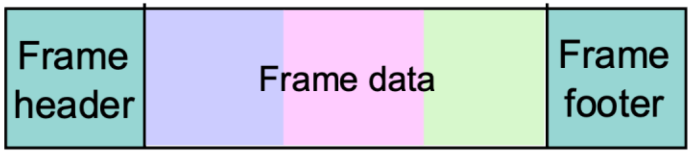
1. **BLOCK** TCP/22
2. **BLOCK** UDP/3389
3. **ALLOW** 1.2.3.4/32
4. **BLOCK** TCP/443
5. **ALLOW** by default



Firewall Example

1. **BLOCK** TCP/22
2. **BLOCK** UDP/3389
3. **ALLOW** 1.2.3.4/32
4. **BLOCK** TCP/443
5. **ALLOW** by default




Frame header

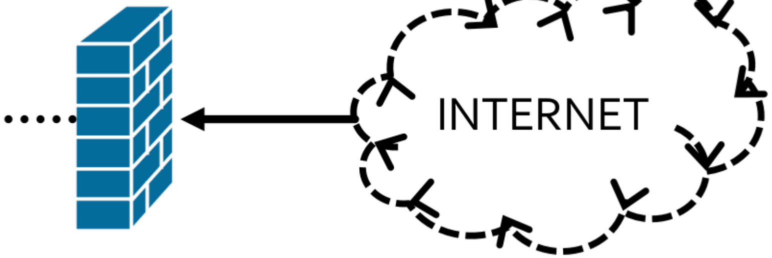
Frame data

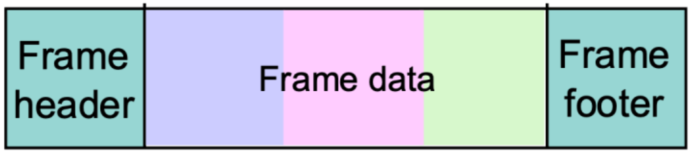
Frame footer

To: 99.99.99.99
TCP/22
XX:X...X:XX

Firewall Example

1. **BLOCK** TCP/22
2. **BLOCK** UDP/3389
3. **ALLOW** 1.2.3.4/32
4. **BLOCK** TCP/443
5. **ALLOW** by default





To: 1.42.13.37
UDP/53
XX:X…X:XX

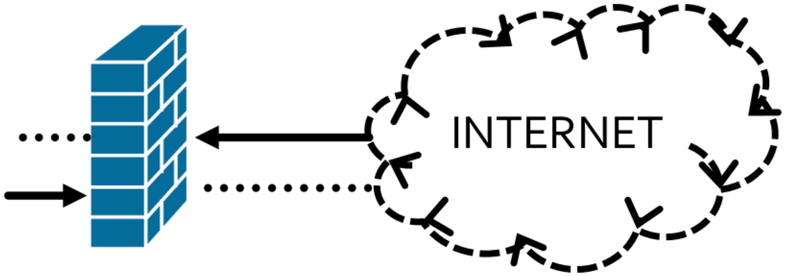
Firewall Implementations

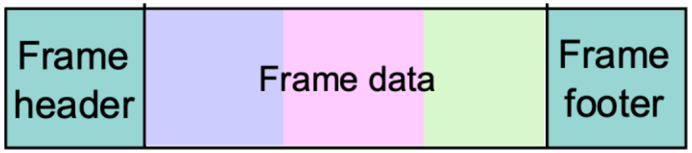
- Blacklisting traffic
  - Match rule? **BLOCK**
- Whitelisting traffic
  - Match rule? **ALLOW**
- Always have a “default rule”

FIREWALL RULES ARE DIRECTIONAL

Firewall Example

1. **BLOCK** inbound to:TCP/22
2. **BLOCK** inbound to:UDP/3389
3. **ALLOW** inbound to:1.2.3.4/32
4. **BLOCK** inbound to:TCP/443
5. **ALLOW** inbound by default
6. **ALLOW** outbound to:TCP/80
7. **ALLOW** outbound to:UDP/53
8. **BLOCK** outbound to:99.99.99.99/32
9. **ALLOW** outbound to:TCP/443
10. **ALLOW** outbound by default



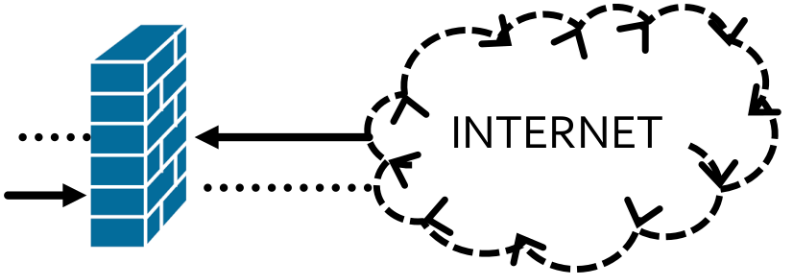


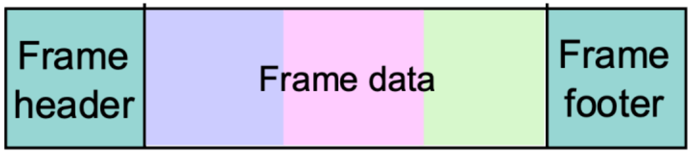
INBOUND

To: 1.2.3.4
TCP/443
XX:X...X:XX
From: 6.7.8.9
TCP/337
XX:X...X:XX

Firewall Example

1. **BLOCK** inbound to:TCP/22
2. **BLOCK** inbound to:UDP/3389
3. **ALLOW** inbound to:1.2.3.4/32
4. **BLOCK** inbound to:TCP/443
5. **ALLOW** inbound by default
6. **ALLOW** outbound to:TCP/80
7. **ALLOW** outbound to:UDP/53
8. **BLOCK** outbound to:99.99.99.99/32
9. **ALLOW** outbound to:TCP/443
10. **ALLOW** outbound by default



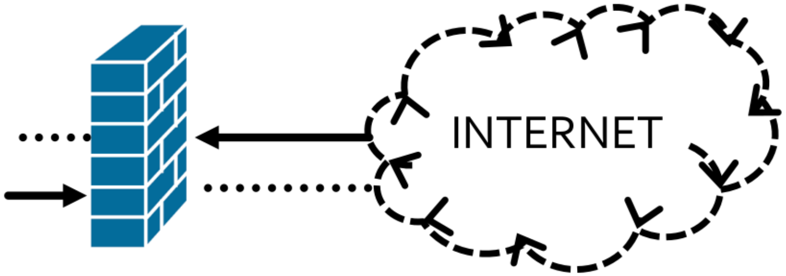


OUTBOUND

To: 1.2.3.4
TCP/443
XX:X…X:XX
From: 6.7.8.9
TCP/337
XX:X…X:XX

Semi-Realistic Firewall Rules

1. **ALLOW** outbound to:UDP/75
2. **BLOCK** inbound to:TCP/43
3. **ALLOW** inbound to:1.2.3.4/32
4. **BLOCK** inbound to:TCP/443
5. **ALLOW** outbound to:TCP/80
6. **BLOCK** outbound to:99.99.99.99/32
7. **ALLOW** outbound to:TCP/443
8. **BLOCK** inbound to:TCP/389
9. **BLOCK** inbound to:TCP/43
10. **ALLOW** outbound to:UDP/53
11. **BLOCK** outbound to:UDP/53
12. **ALLOW** outbound by default
13. **BLOCK** inbound to:TCP/243
14. **BLOCK** inbound to:TCP/443
15. **BLOCK** inbound to:TCP/694
16. **BLOCK** outbound to:UDP/1111
17. **BLOCK** outbound to:UDP/435
18. **BLOCK** outbound to:UDP/3943
19. **BLOCK** outbound to:UDP/954
20. **ALLOW** inbound by default

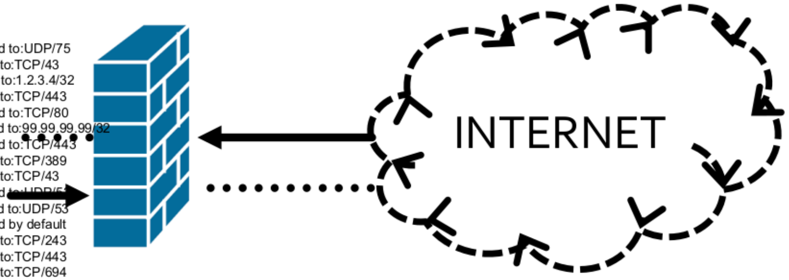


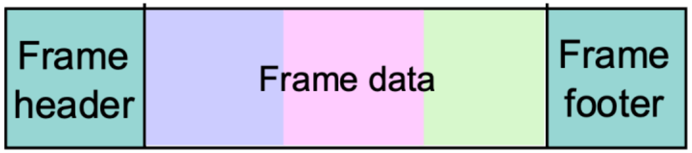
Realistic Firewall Rules

1. **ALLOW** outbound to:UDP/75
2. **BLOCK** inbound to:TCP/43
3. **ALLOW** inbound to:1.2.3.4/32
4. **BLOCK** inbound to:TCP/443
5. **ALLOW** outbound to:TCP/80
6. **BLOCK** outbound to:99.99.99.99/32
7. **ALLOW** outbound to:TCP/443
8. **BLOCK** inbound to:TCP/389
9. **BLOCK** inbound to:TCP/43
10. **ALLOW** outbound to:UDP/53
11. **BLOCK** outbound to:UDP/53
12. **ALLOW** outbound by default
13. **BLOCK** inbound to:TCP/243
14. **BLOCK** inbound to:TCP/443
15. **BLOCK** inbound to:TCP/694
16. **BLOCK** outbound to:UDP/1111
17. **BLOCK** outbound to:UDP/435
18. **BLOCK** outbound to:UDP/3943
19. **BLOCK** outbound to:UDP/954
20. **ALLOW** inbound by default
21. **ALLOW** outbound to:UDP/75
22. **BLOCK** inbound to:TCP/43
23. **ALLOW** inbound to:1.2.3.4/32
24. **BLOCK** inbound to:TCP/443
25. **ALLOW** outbound to:TCP/80
26. **BLOCK** outbound to:99.99.99.99/32
27. **ALLOW** outbound to:TCP/443
28. **BLOCK** inbound to:TCP/389
29. **BLOCK** inbound to:TCP/43
30. **ALLOW** outbound to:UDP/53
31. **BLOCK** outbound to:UDP/53
32. **ALLOW** outbound by default
33. **BLOCK** inbound to:TCP/243
34. **BLOCK** inbound to:TCP/443
35. **BLOCK** inbound to:TCP/694
36. **BLOCK** outbound to:UDP/1111
37. **BLOCK** outbound to:UDP/435
38. **BLOCK** outbound to:UDP/3943
39. **BLOCK** outbound to:UDP/954
40. **ALLOW** inbound by default
41. **ALLOW** outbound to:UDP/75
42. **BLOCK** inbound to:TCP/43
43. **ALLOW** inbound to:1.2.3.4/32
44. **BLOCK** inbound to:TCP/443
45. **ALLOW** outbound to:TCP/80
46. **BLOCK** outbound to:99.99.99.99/32
47. **ALLOW** outbound to:TCP/443
48. **BLOCK** inbound to:TCP/389
49. **BLOCK** inbound to:TCP/43
50. **ALLOW** outbound to:UDP/53
51. **BLOCK** outbound to:UDP/53
52. **ALLOW** outbound by default
53. **BLOCK** inbound to:TCP/243
54. **BLOCK** inbound to:TCP/443
55. **BLOCK** inbound to:TCP/694
56. **BLOCK** outbound to:UDP/1111
57. **BLOCK** outbound to:UDP/435
58. **BLOCK** outbound to:UDP/3943
59. **BLOCK** outbound to:UDP/954
60. **ALLOW** inbound by default

1. **ALLOW** outbound to:UDP/75
2. **BLOCK** inbound to:TCP/43
3. **ALLOW** inbound to:1.2.3.4/32
4. **BLOCK** inbound to:TCP/443
5. **ALLOW** outbound to:TCP/80
6. **BLOCK** outbound to:99.99.99.99/32
7. **ALLOW** outbound to:TCP/443
8. **BLOCK** inbound to:TCP/389
9. **BLOCK** inbound to:TCP/43
10. **ALLOW** outbound to:UDP/53
11. **BLOCK** outbound to:UDP/53
12. **ALLOW** outbound by default
13. **BLOCK** inbound to:TCP/243
14. **BLOCK** inbound to:TCP/443
15. **BLOCK** inbound to:TCP/694
16. **BLOCK** outbound to:UDP/1111
17. **BLOCK** outbound to:UDP/435
18. **BLOCK** outbound to:UDP/3943
19. **BLOCK** outbound to:UDP/954
20. **ALLOW** inbound by default
21. **ALLOW** outbound to:UDP/75
22. **BLOCK** inbound to:TCP/43
23. **ALLOW** inbound to:1.2.3.4/32
24. **BLOCK** inbound to:TCP/443
25. **ALLOW** outbound to:TCP/80
26. **BLOCK** outbound to:99.99.99.99/32
27. **ALLOW** outbound to:TCP/443
28. **BLOCK** inbound to:TCP/389
29. **BLOCK** inbound to:TCP/43
30. **ALLOW** outbound to:UDP/53
31. **BLOCK** outbound to:UDP/53
32. **ALLOW** outbound by default
33. **BLOCK** inbound to:TCP/243
34. **BLOCK** inbound to:TCP/443
35. **BLOCK** inbound to:TCP/694
36. **BLOCK** outbound to:UDP/1111
37. **BLOCK** outbound to:UDP/435
38. **BLOCK** outbound to:UDP/3943
39. **BLOCK** outbound to:UDP/954
40. **ALLOW** inbound by default
41. **ALLOW** outbound to:UDP/75
42. **BLOCK** inbound to:TCP/43
43. **ALLOW** inbound to:1.2.3.4/32
44. **BLOCK** inbound to:TCP/443
45. **ALLOW** outbound to:TCP/80
46. **BLOCK** outbound to:99.99.99.99/32
47. **ALLOW** outbound to:TCP/443
48. **BLOCK** inbound to:TCP/389
49. **BLOCK** inbound to:TCP/43
50. **ALLOW** outbound to:UDP/53
51. **BLOCK** outbound to:UDP/53
52. **ALLOW** outbound by default
53. **BLOCK** inbound to:TCP/243
54. **BLOCK** inbound to:TCP/443
55. **BLOCK** inbound to:TCP/694
56. **BLOCK** outbound to:UDP/1111
57. **BLOCK** outbound to:UDP/435
58. **BLOCK** outbound to:UDP/3943
59. **BLOCK** outbound to:UDP/954
60. **ALLOW** inbound by default

1. **ALLOW** outbound to:UDP/75
2. **BLOCK** inbound to:TCP/43
3. **ALLOW** inbound to:1.2.3.4/32
4. **BLOCK** inbound to:TCP/443
5. **ALLOW** outbound to:TCP/80
6. **BLOCK** outbound to:99.99.99.99/32
7. **ALLOW** outbound to:TCP/443
8. **BLOCK** inbound to:TCP/389
9. **BLOCK** inbound to:TCP/43
10. **ALLOW** outbound to:UDP/53
11. **BLOCK** outbound to:UDP/53
12. **ALLOW** outbound by default
13. **BLOCK** inbound to:TCP/243
14. **BLOCK** inbound to:TCP/443
15. **BLOCK** inbound to:TCP/694
16. **BLOCK** outbound to:UDP/1111
17. **BLOCK** outbound to:UDP/435
18. **BLOCK** outbound to:UDP/3943
19. **BLOCK** outbound to:UDP/954
20. **ALLOW** inbound by default
21. **ALLOW** outbound to:UDP/75
22. **BLOCK** inbound to:TCP/43
23. **ALLOW** inbound to:1.2.3.4/32
24. **BLOCK** inbound to:TCP/443
25. **ALLOW** outbound to:TCP/80
26. **BLOCK** outbound to:99.99.99.99/32
27. **ALLOW** outbound to:TCP/443
28. **BLOCK** inbound to:TCP/389
29. **BLOCK** inbound to:TCP/43
30. **ALLOW** outbound to:UDP/53
31. **BLOCK** outbound to:UDP/53
32. **ALLOW** outbound by default
33. **BLOCK** inbound to:TCP/243
34. **BLOCK** inbound to:TCP/443
35. **BLOCK** inbound to:TCP/694
36. **BLOCK** outbound to:UDP/1111
37. **BLOCK** outbound to:UDP/435
38. **BLOCK** outbound to:UDP/3943
39. **BLOCK** outbound to:UDP/954
40. **ALLOW** inbound by default
41. **ALLOW** outbound to:UDP/75
42. **BLOCK** inbound to:TCP/43
43. **ALLOW** inbound to:1.2.3.4/32
44. **BLOCK** inbound to:TCP/443
45. **ALLOW** outbound to:TCP/80
46. **BLOCK** outbound to:99.99.99.99/32
47. **ALLOW** outbound to:TCP/443
48. **BLOCK** inbound to:TCP/389
49. **BLOCK** inbound to:TCP/43
50. **ALLOW** outbound to:UDP/53
51. **BLOCK** outbound to:UDP/53
52. **ALLOW** outbound by default
53. **BLOCK** inbound to:TCP/243
54. **BLOCK** inbound to:TCP/443
55. **BLOCK** inbound to:TCP/694
56. **BLOCK** outbound to:UDP/1111
57. **BLOCK** outbound to:UDP/435
58. **BLOCK** outbound to:UDP/3943
59. **BLOCK** outbound to:UDP/954
60. **ALLOW** inbound by default



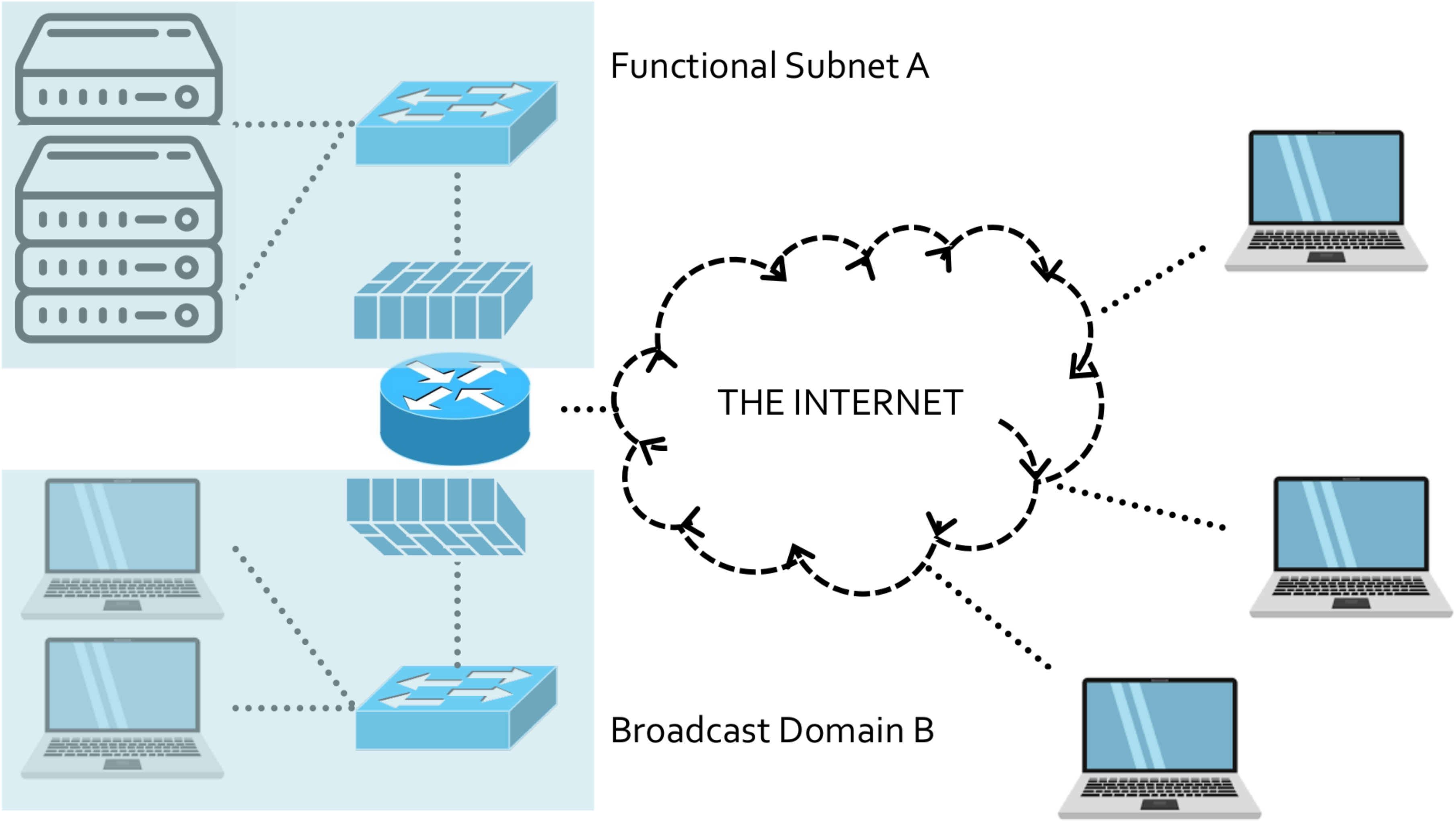


OUTBOUND

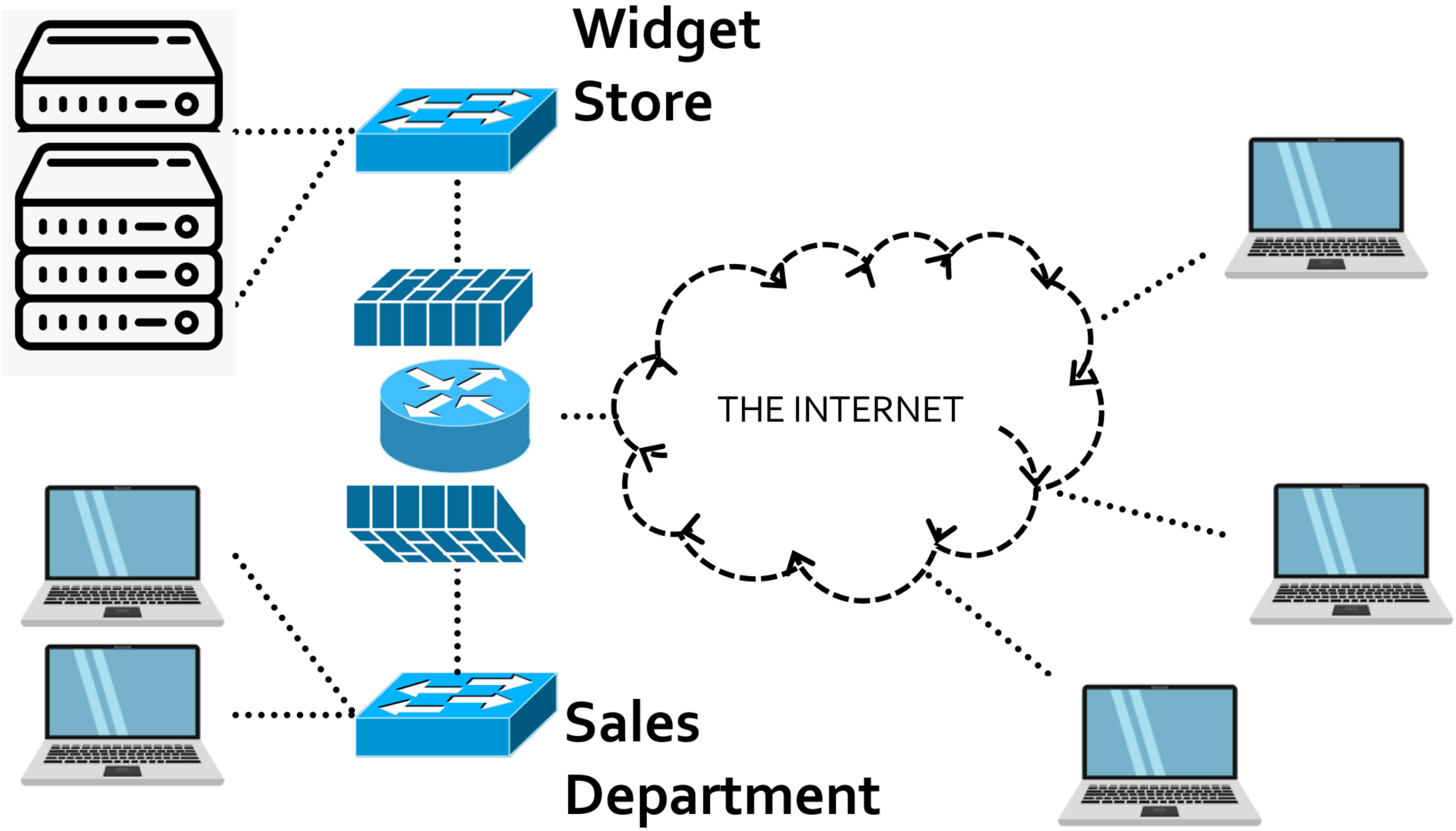
To: 3.43.43.53
TCP/133
XX:X…X:XX

From: 48.5.84.66
TCP/4935
XX:X…X:XX

Functional Subnetting



What might we setup?

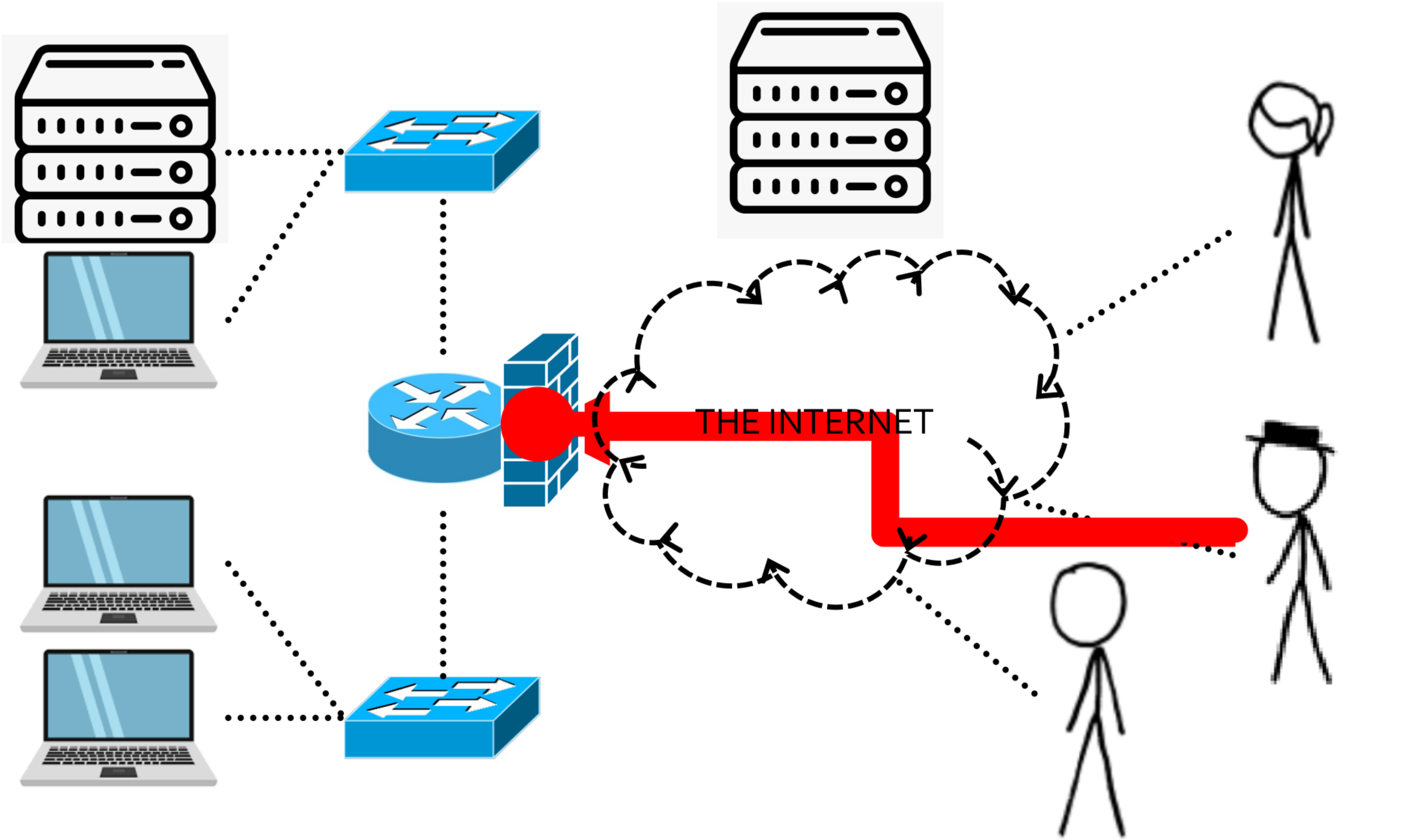


Denial of Service (DoS) Attacks

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

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

Naïve DoS



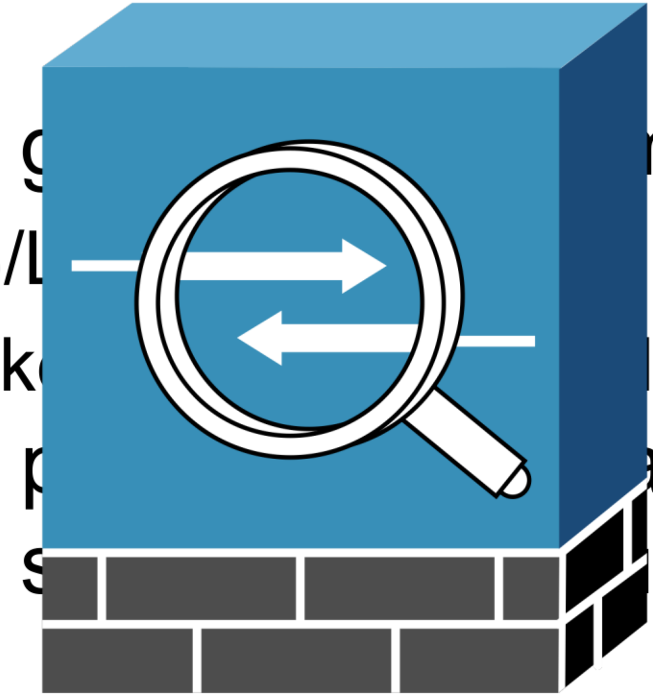
Intrusion Detection System (IDS)

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 <u>Detection</u> System (IDS)** is a network ***monitoring*** component that is able to ***watch*** for signs of maliciousness.



- Capable of g nplex rules
  - Beyond L3/L
  - "Deep Pack I)
- Capable of p atching
- Capable of s lti-flow patterns

ACCESS
OGISTIC
ATCH
SONAR
SPHERE
ENT
S SUBMARINE

FX

Intrusion Prevention System (IPS)

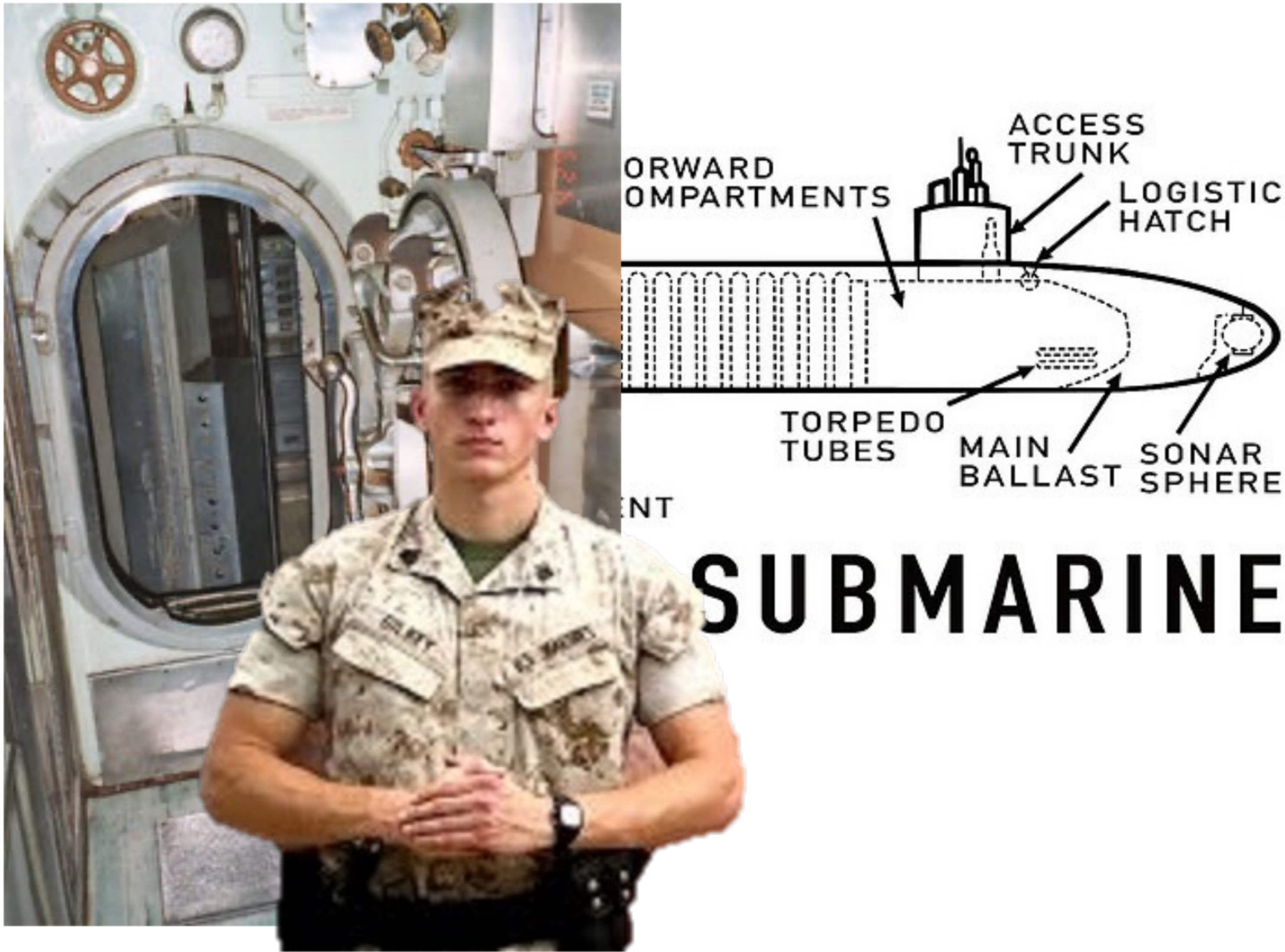
An **Intrusion Prevention System (IPS)** is a type of IDS which is able to actively block maliciousness when found.

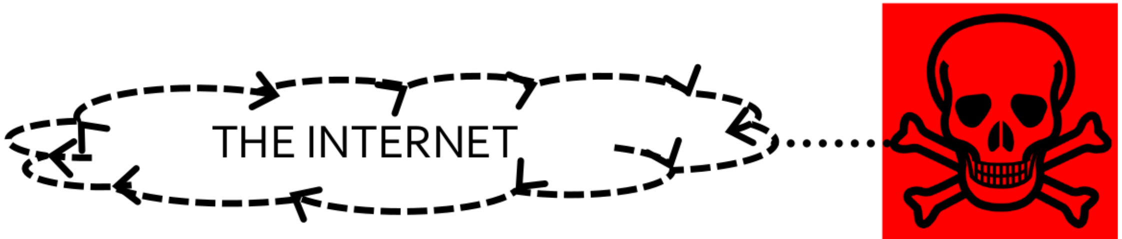
- Capable of granular and complex rules
  - Beyond L2/L3 (TCP/IP) headers
  - “Deep Packet Inspection” (DPI)
- Capable of pattern/regex matching
- Capable of searching for multi-flow patterns

Intrusion Prevention System (IPS)

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

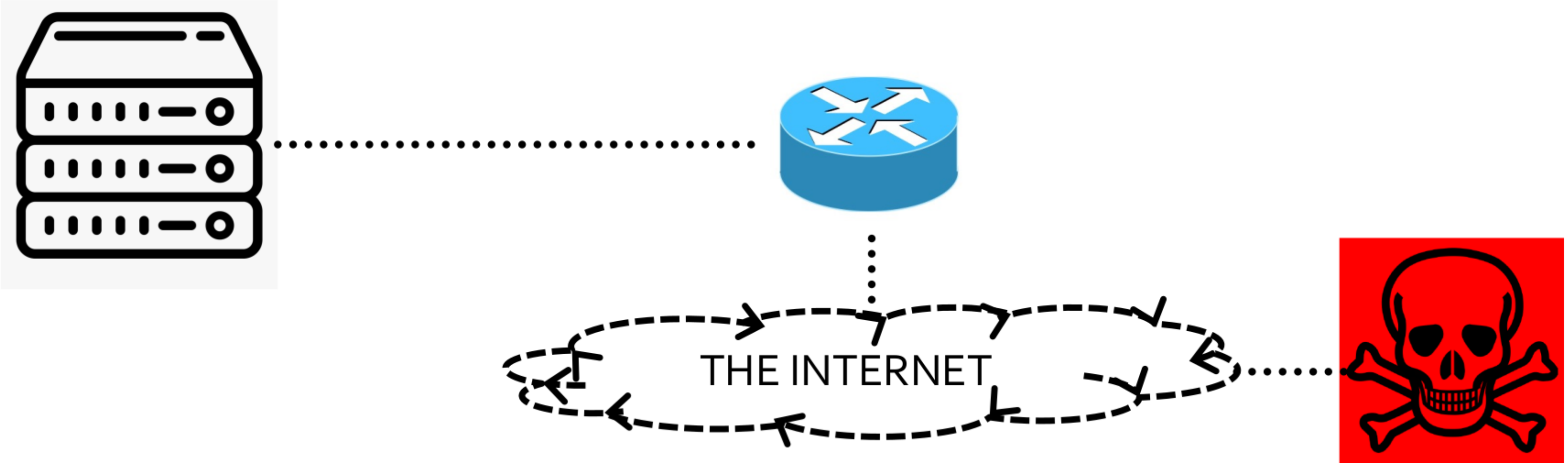
- Capable of granular and complex rules
  - Beyond L2/L3 (TCP/IP) headers
  - “Deep Packet Inspection” (DPI)
- Capable of pattern/regex matching
- Capable of searching for multi-flow patterns


ACCESS TRUNK
ORWARD OMPARTMENTS
LOGISTIC HATCH
TORPEDO TUBES
MAIN BALLAST
SONAR SPHERE
NT
SUBMARINE

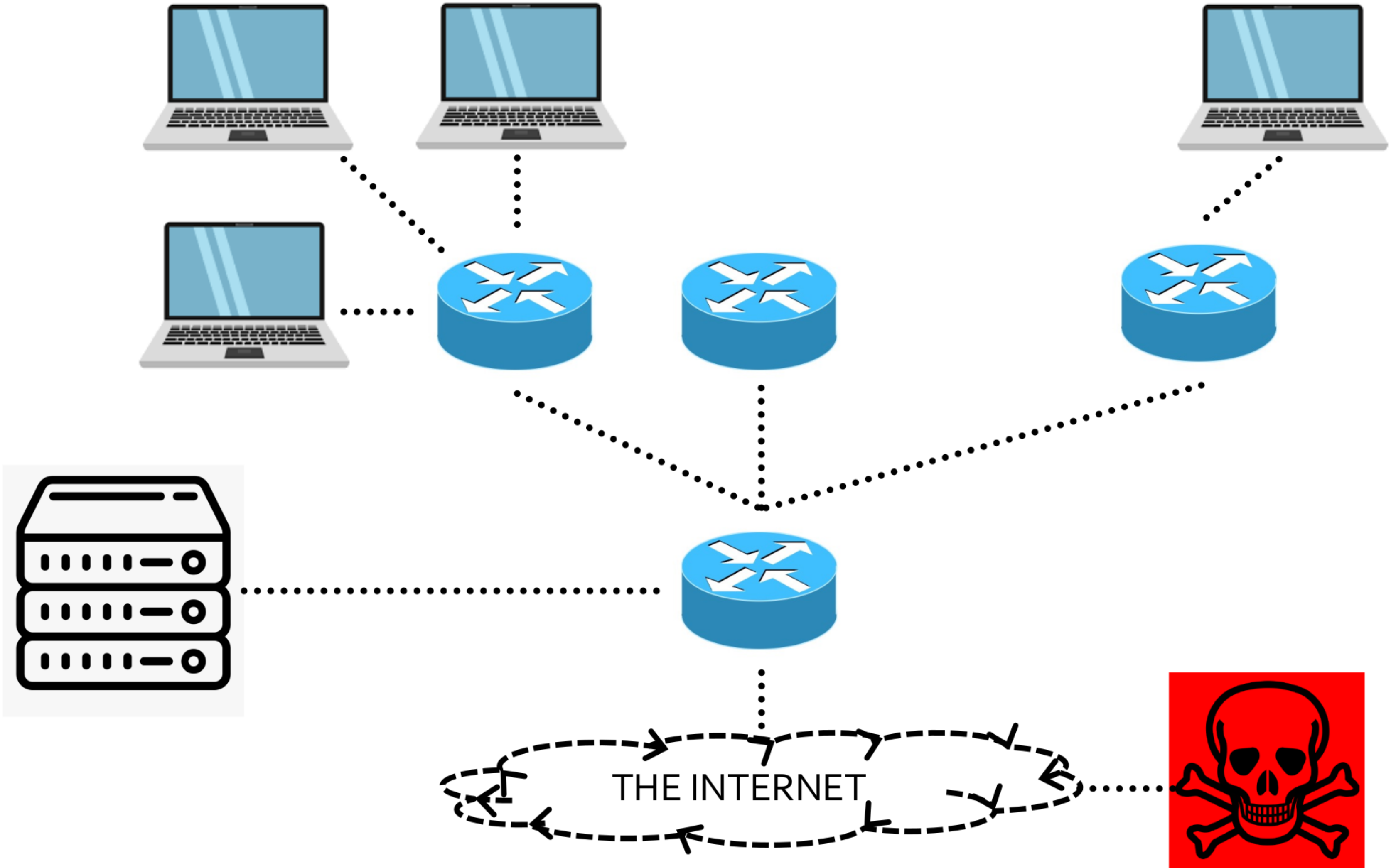


THE INTERNET

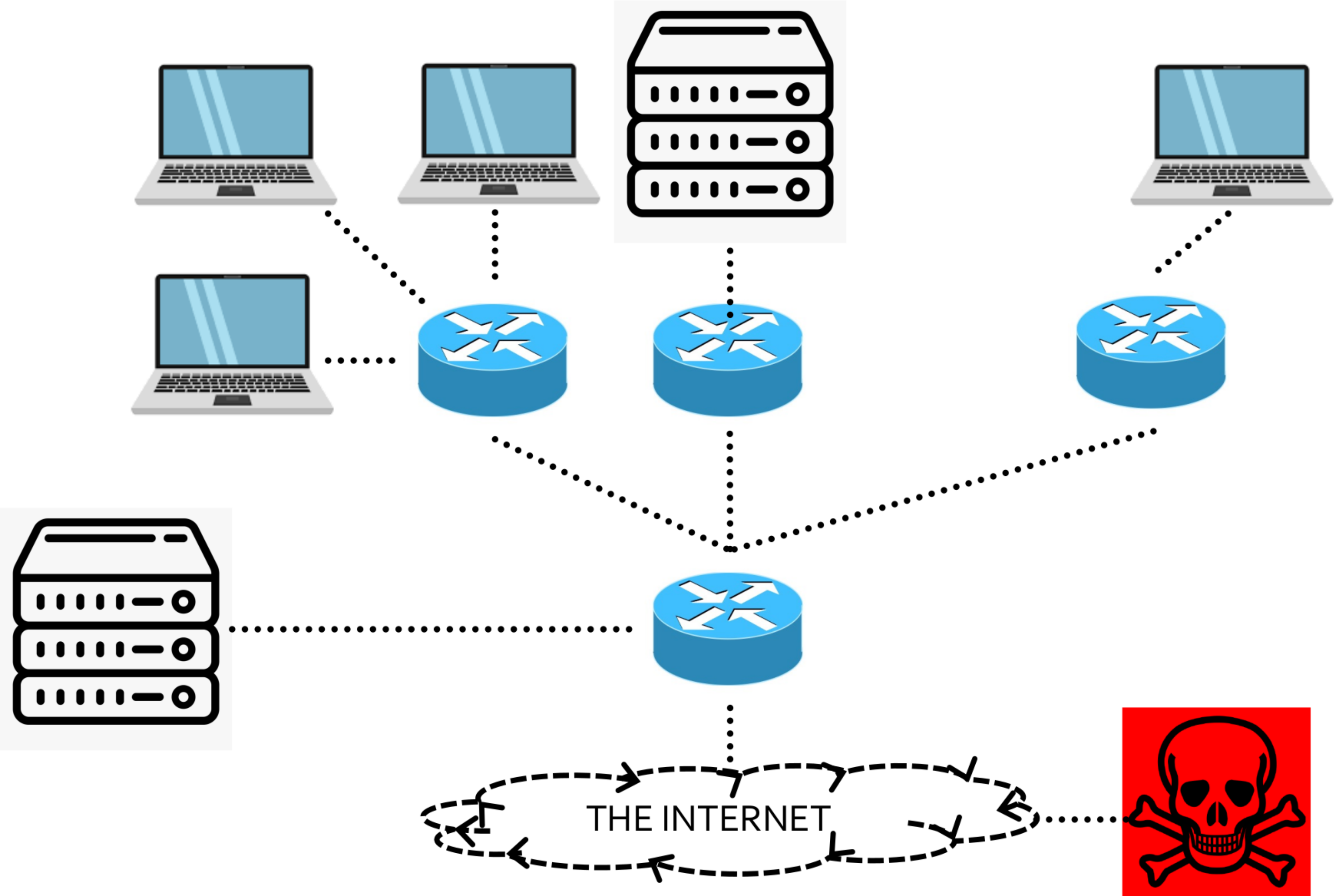
Network Enumeration (ext)



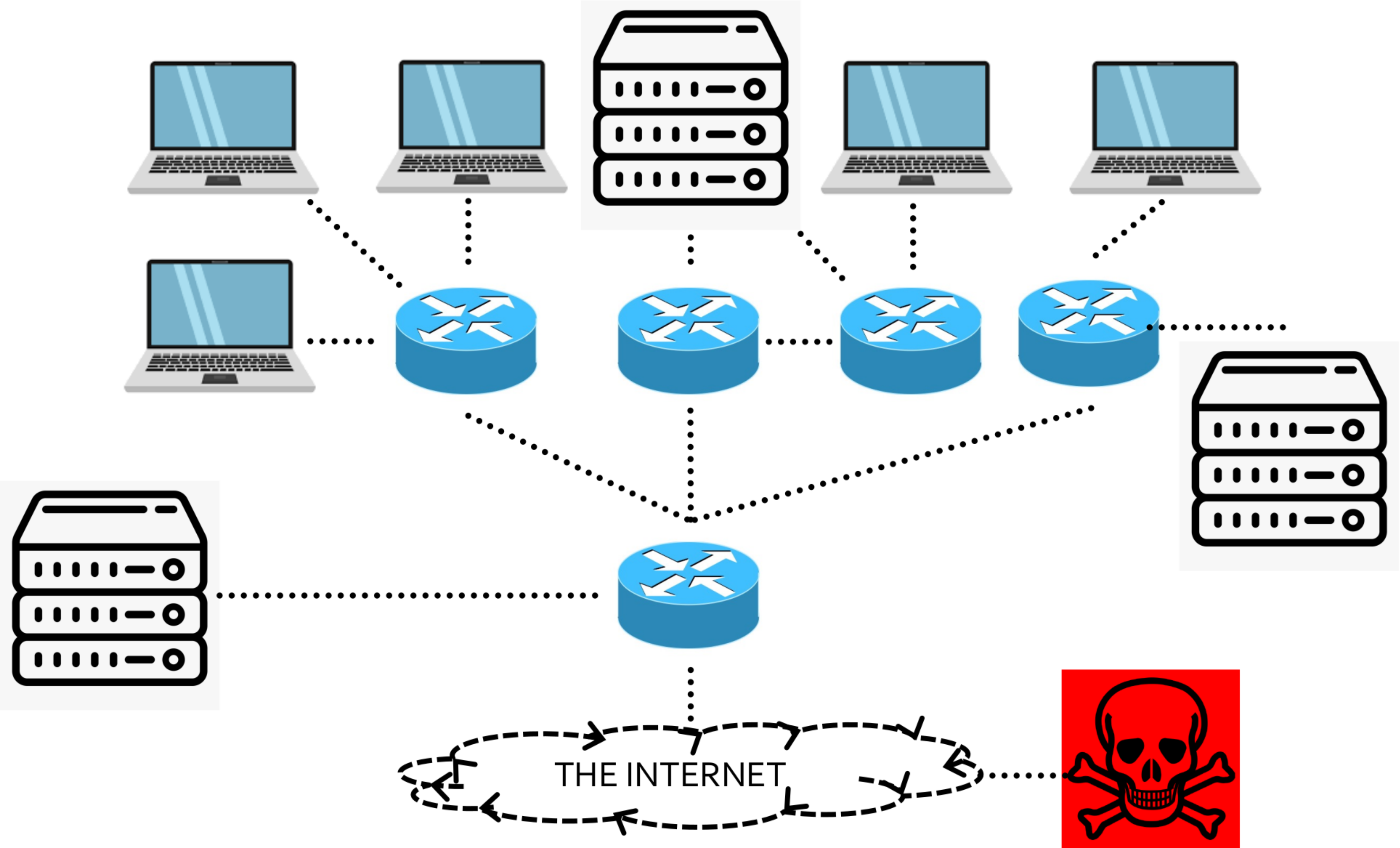
Network Enumeration (ext)



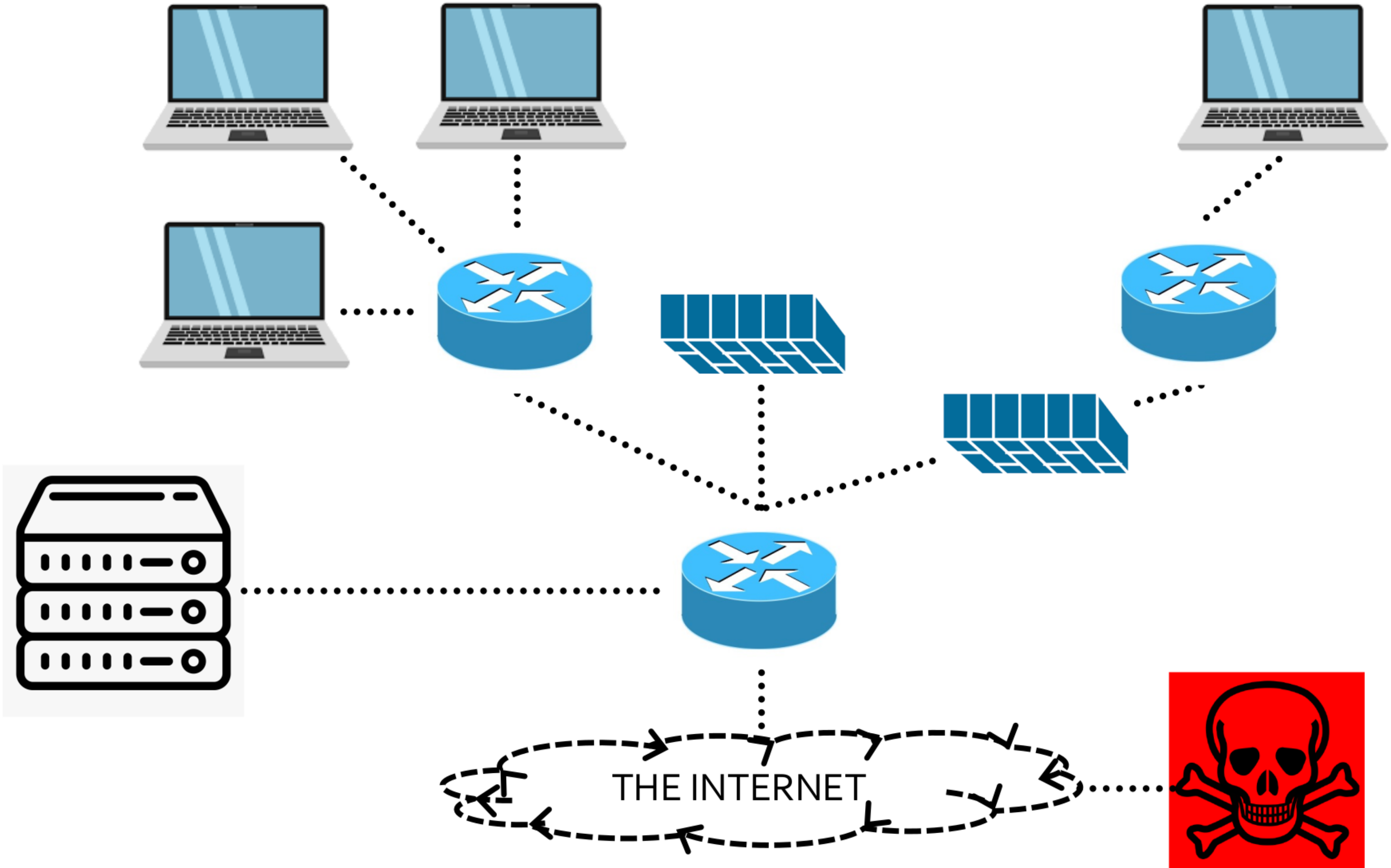
Network Enumeration (ext)



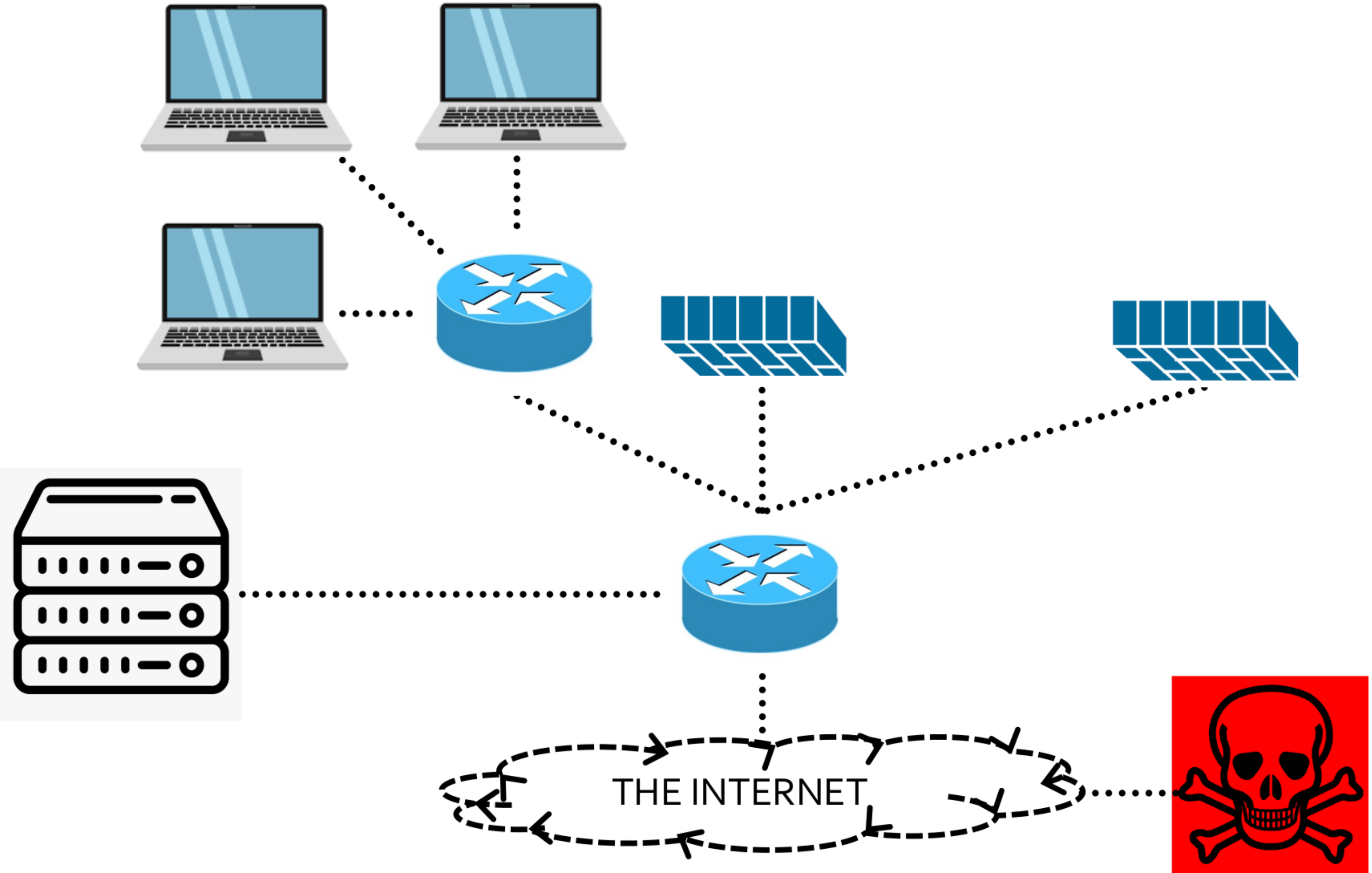
Network Enumeration (ext)



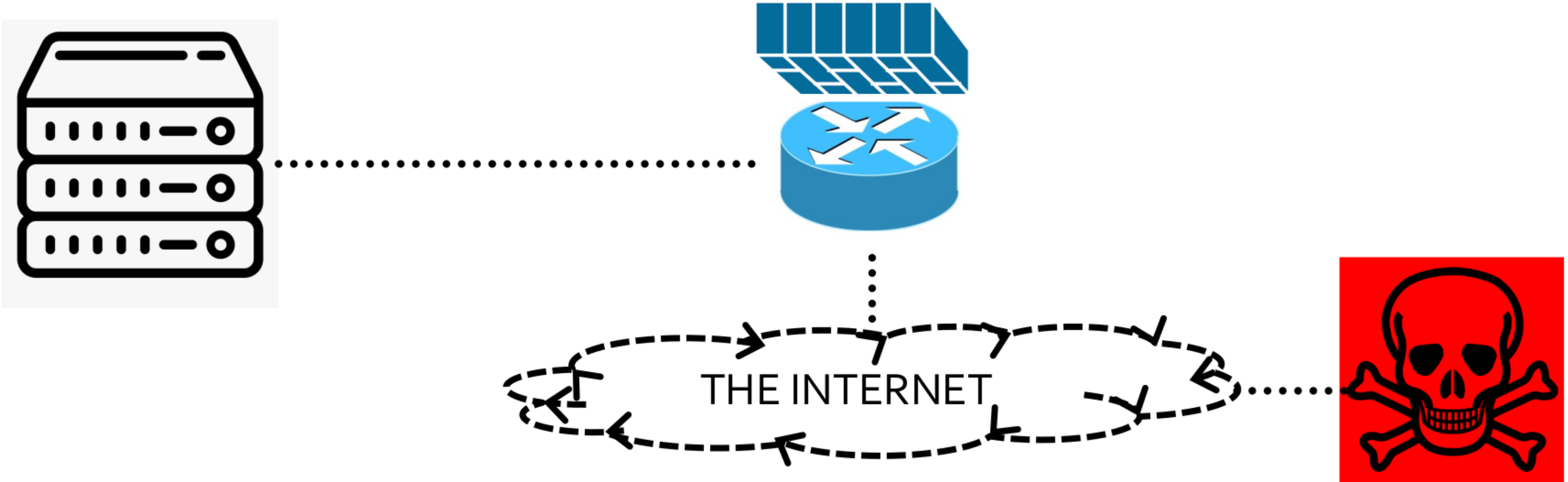
Firewall Defenses



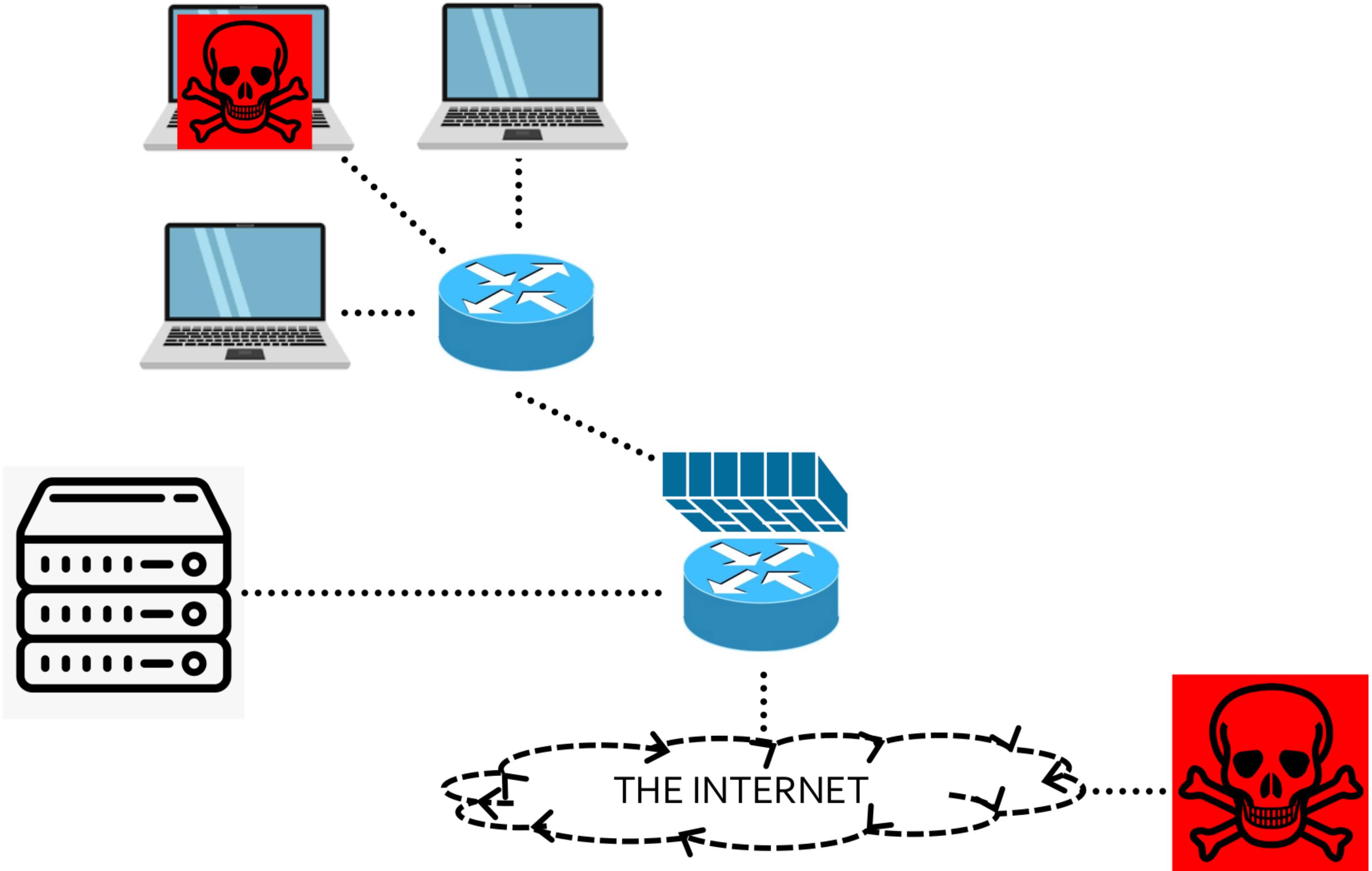
Firewall Defenses



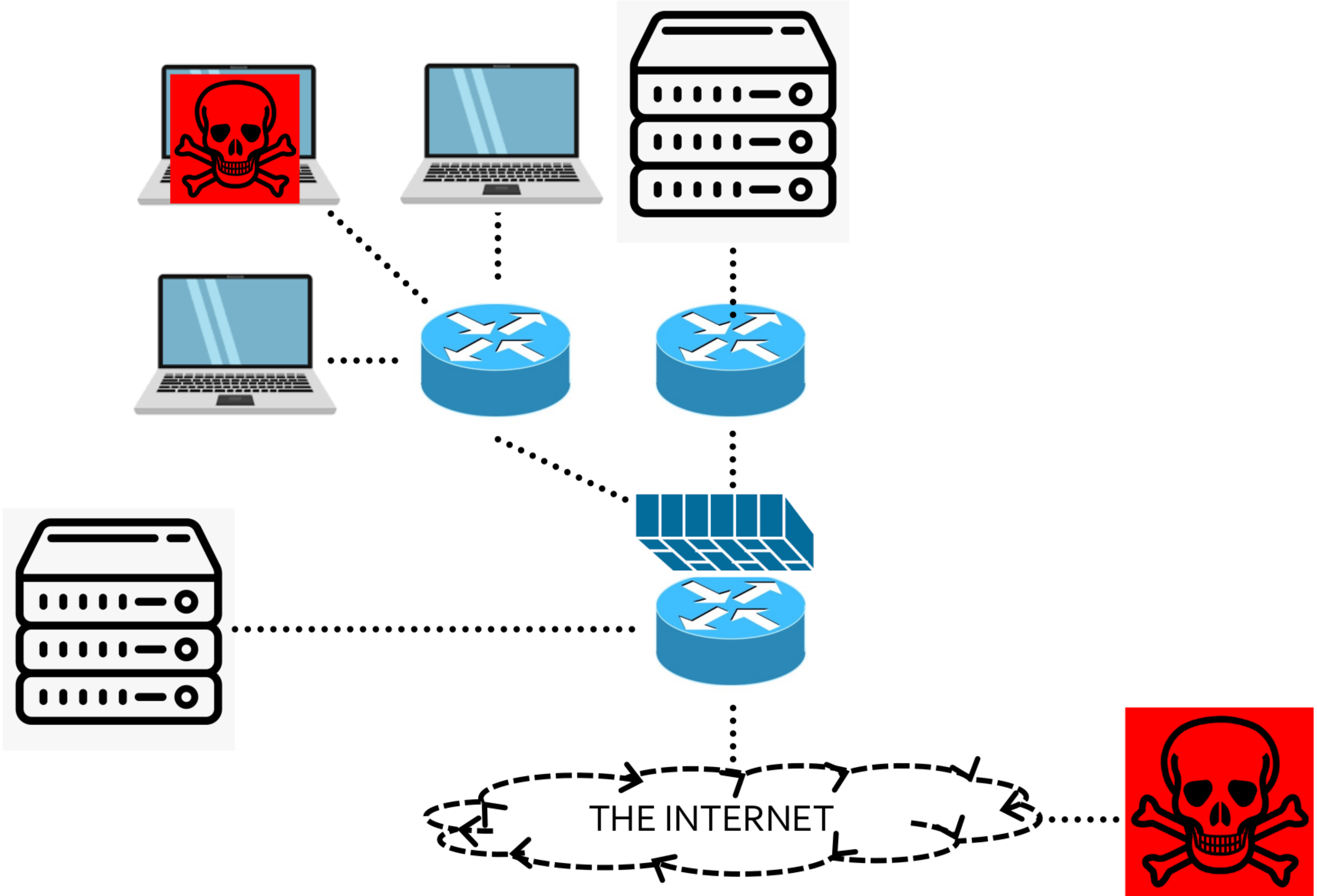
Firewall Defenses



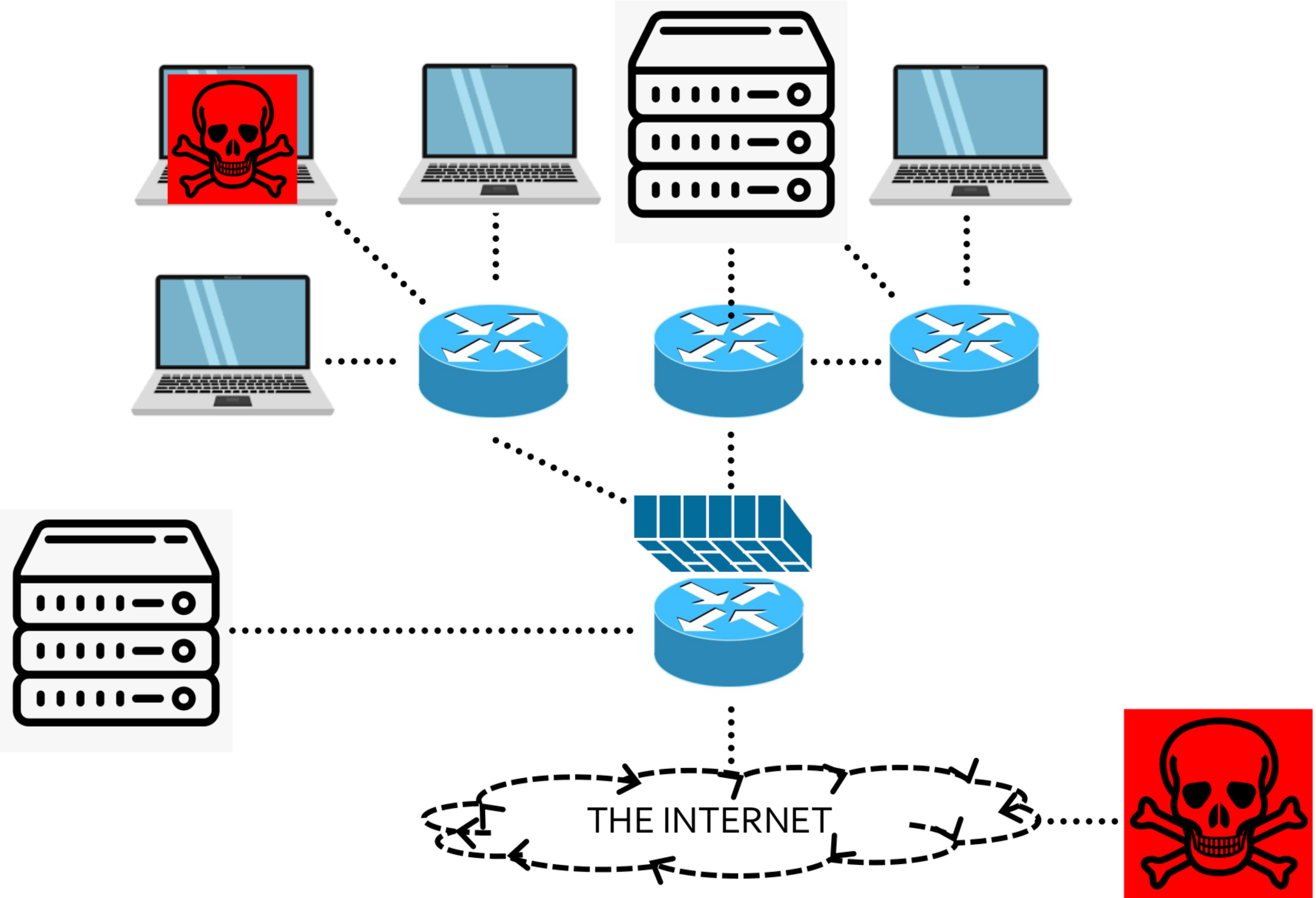
Network Enumeration (int)



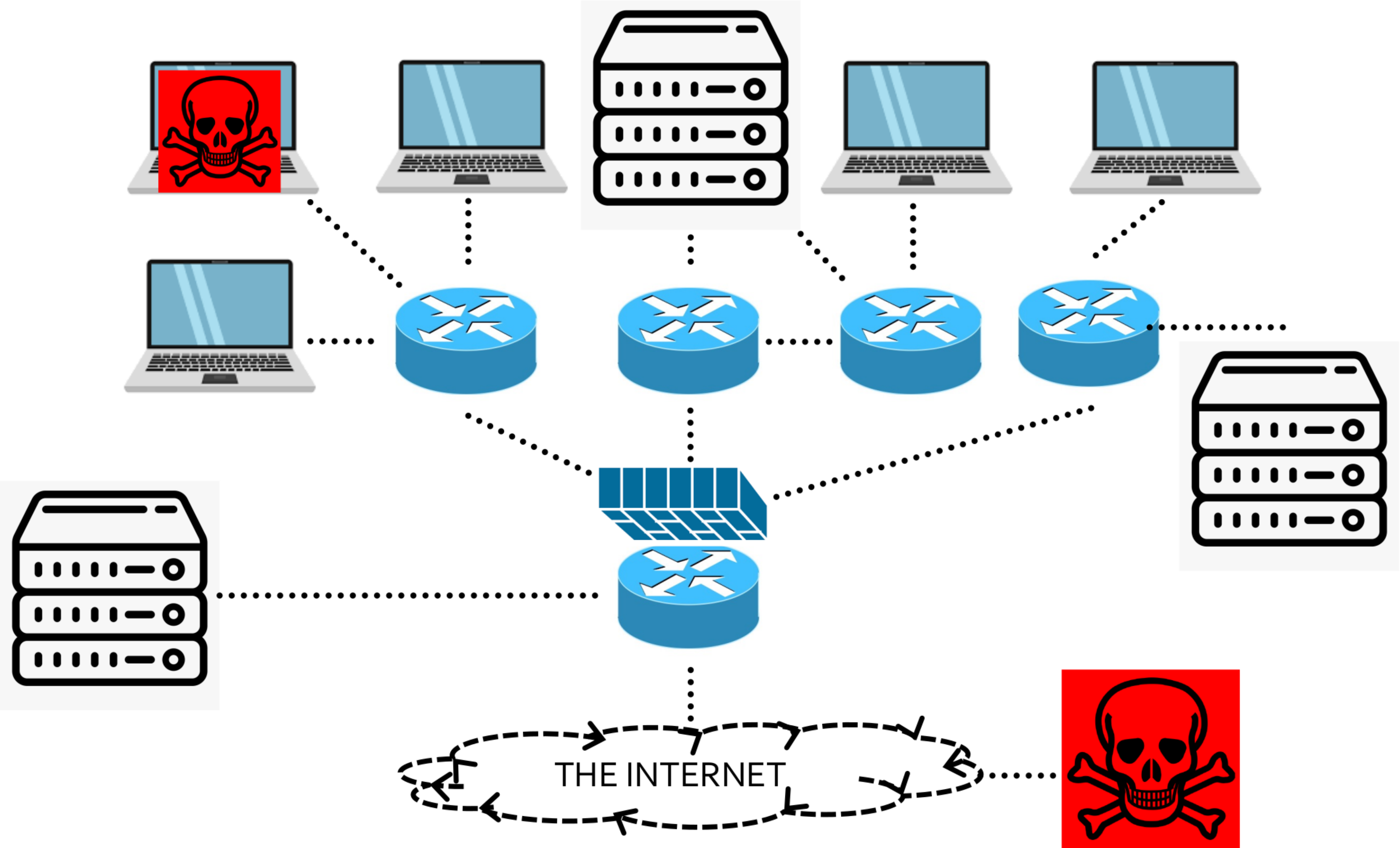
Network Enumeration (int)



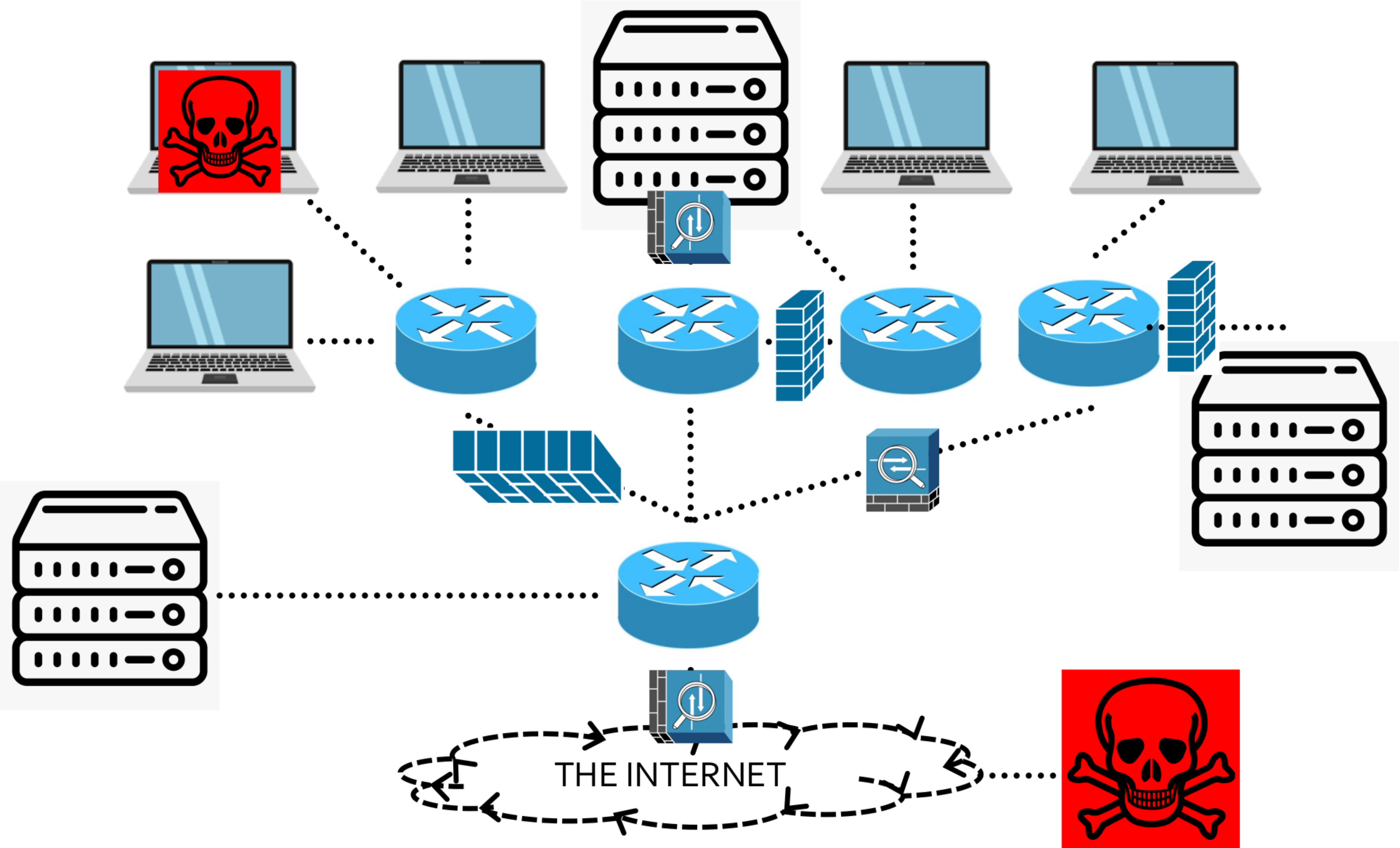
Network Enumeration (int)



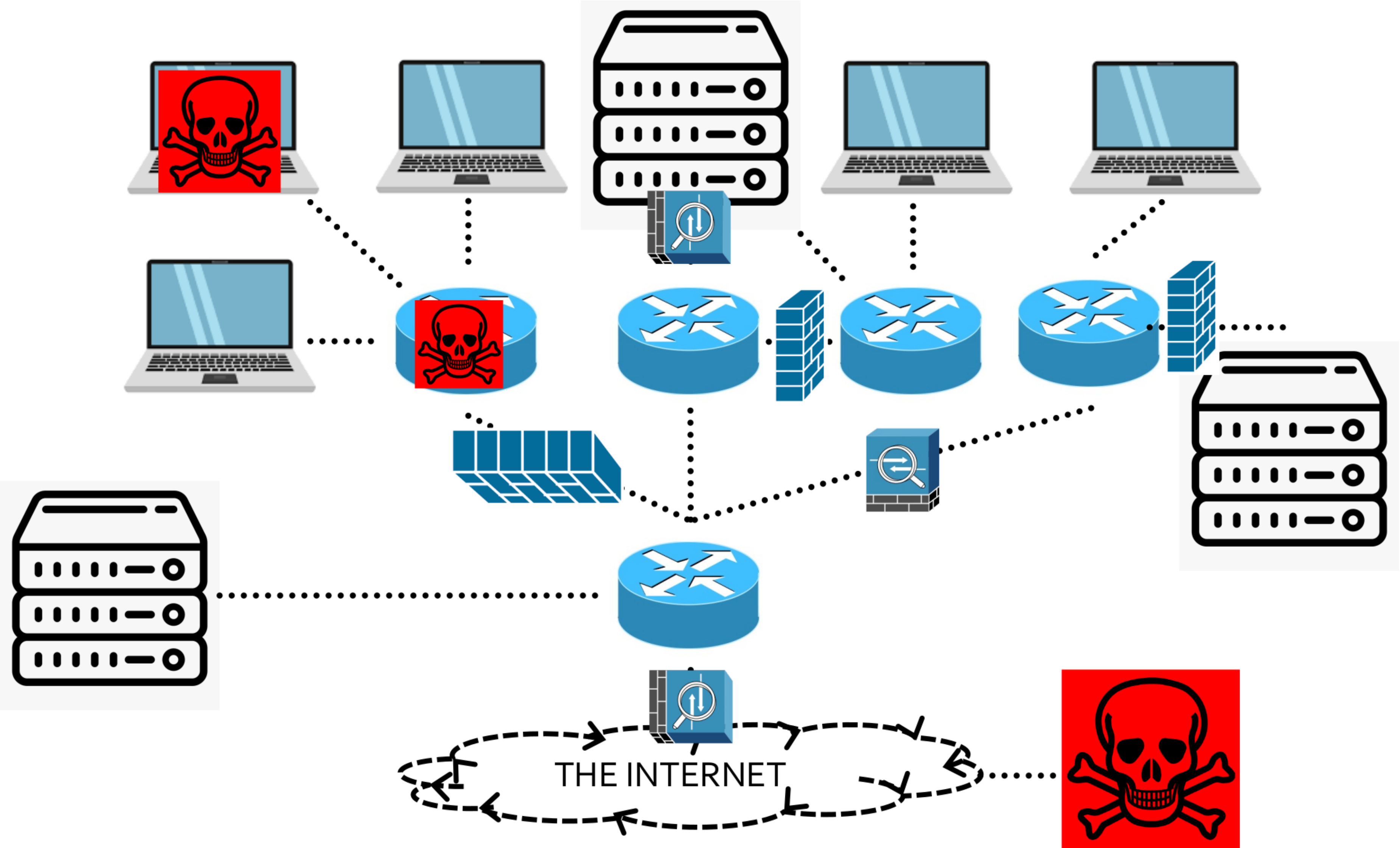
Network Enumeration (int)



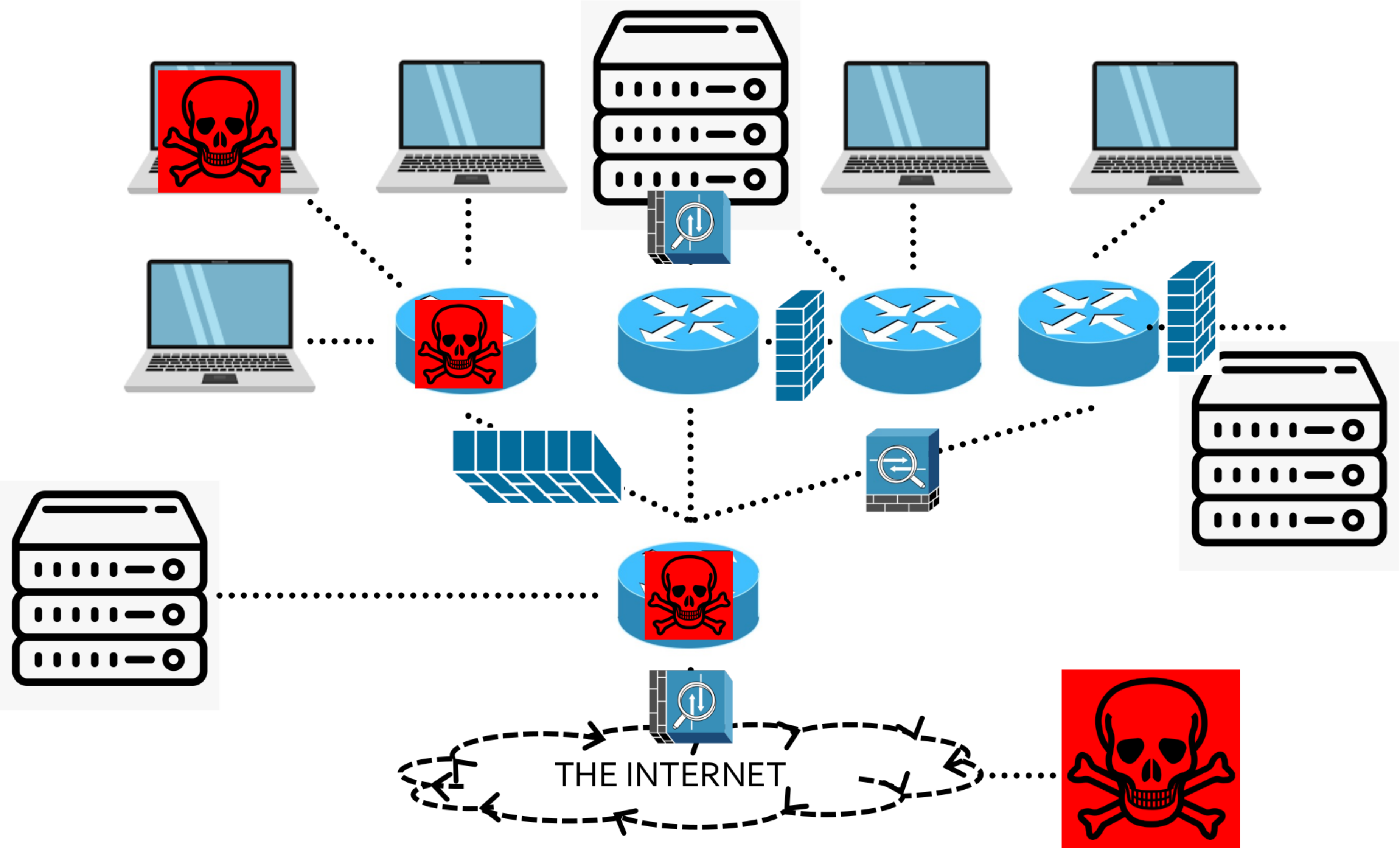
Network Traversal/ Lateral Movement



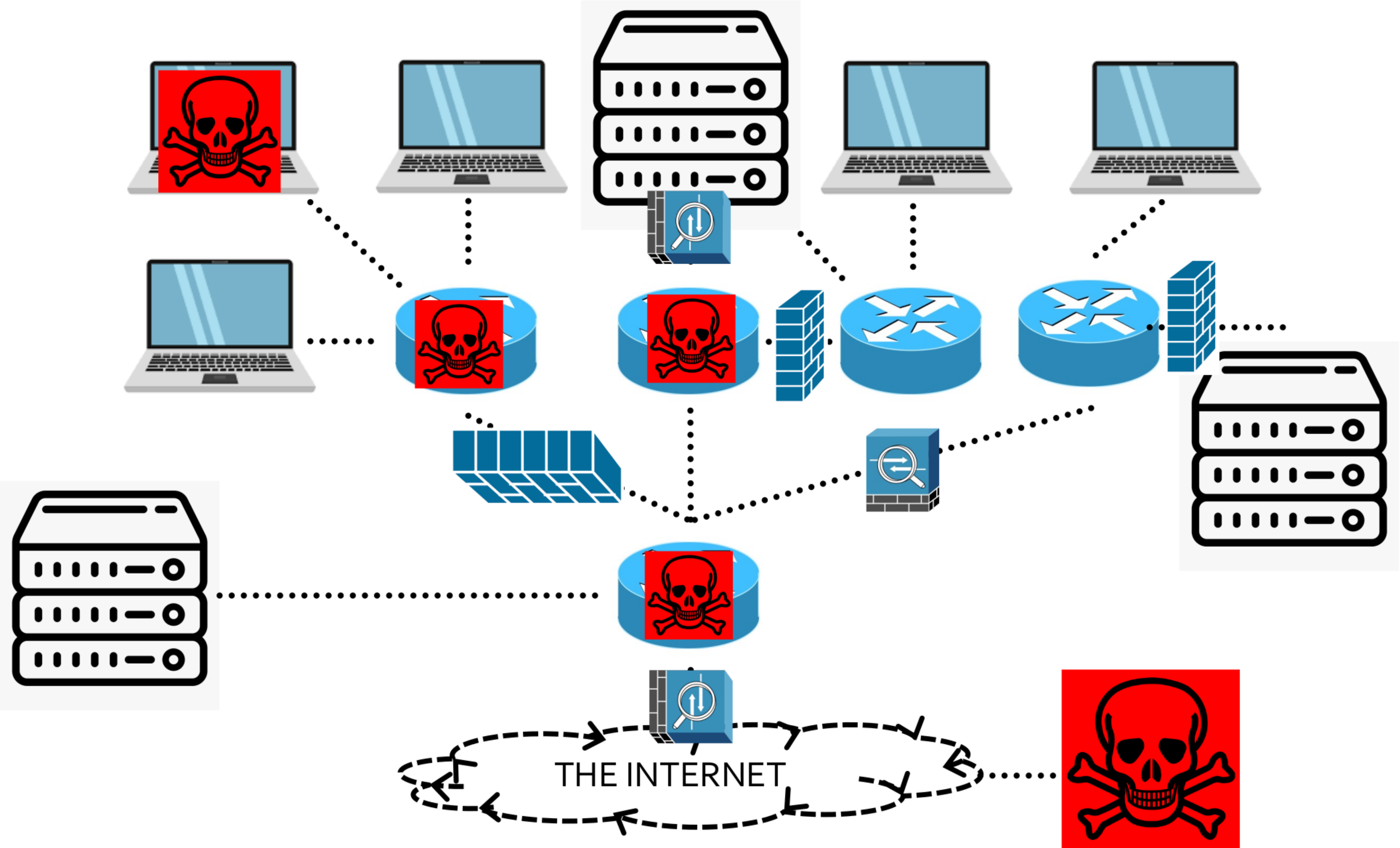
Network Traversal/ Lateral Movement



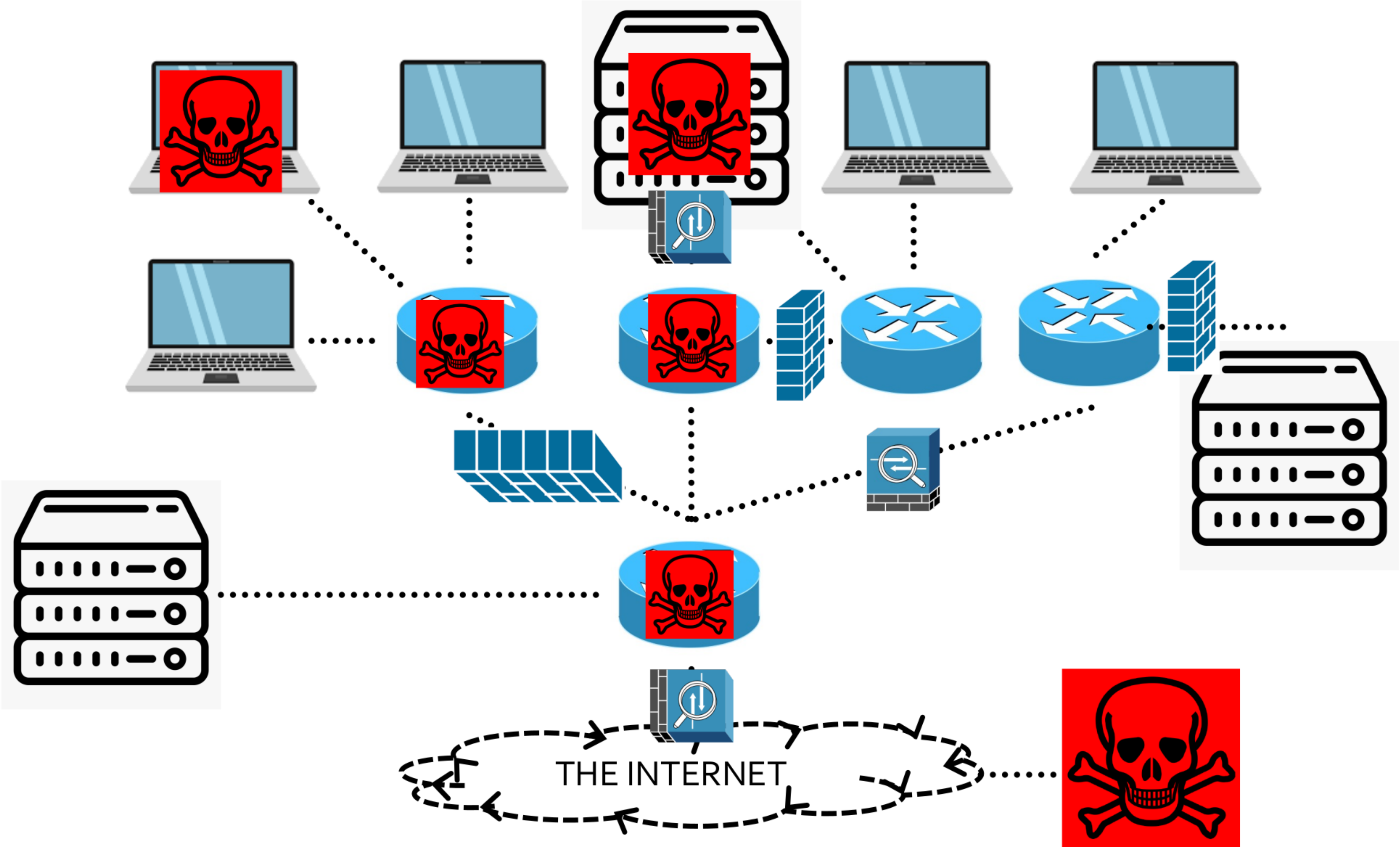
Network Traversal/ Lateral Movement



Network Traversal/ Lateral Movement



Network Traversal/ Lateral Movement


THE INTERNET