TRYHACKME · HANDS-ON NETWORKING LAB

Extending the Network: Understanding the Security Boundary

“A secure network is not simply a collection of devices connected together. It is a system of controlled communication, trust boundaries, routing decisions, and security policies.”

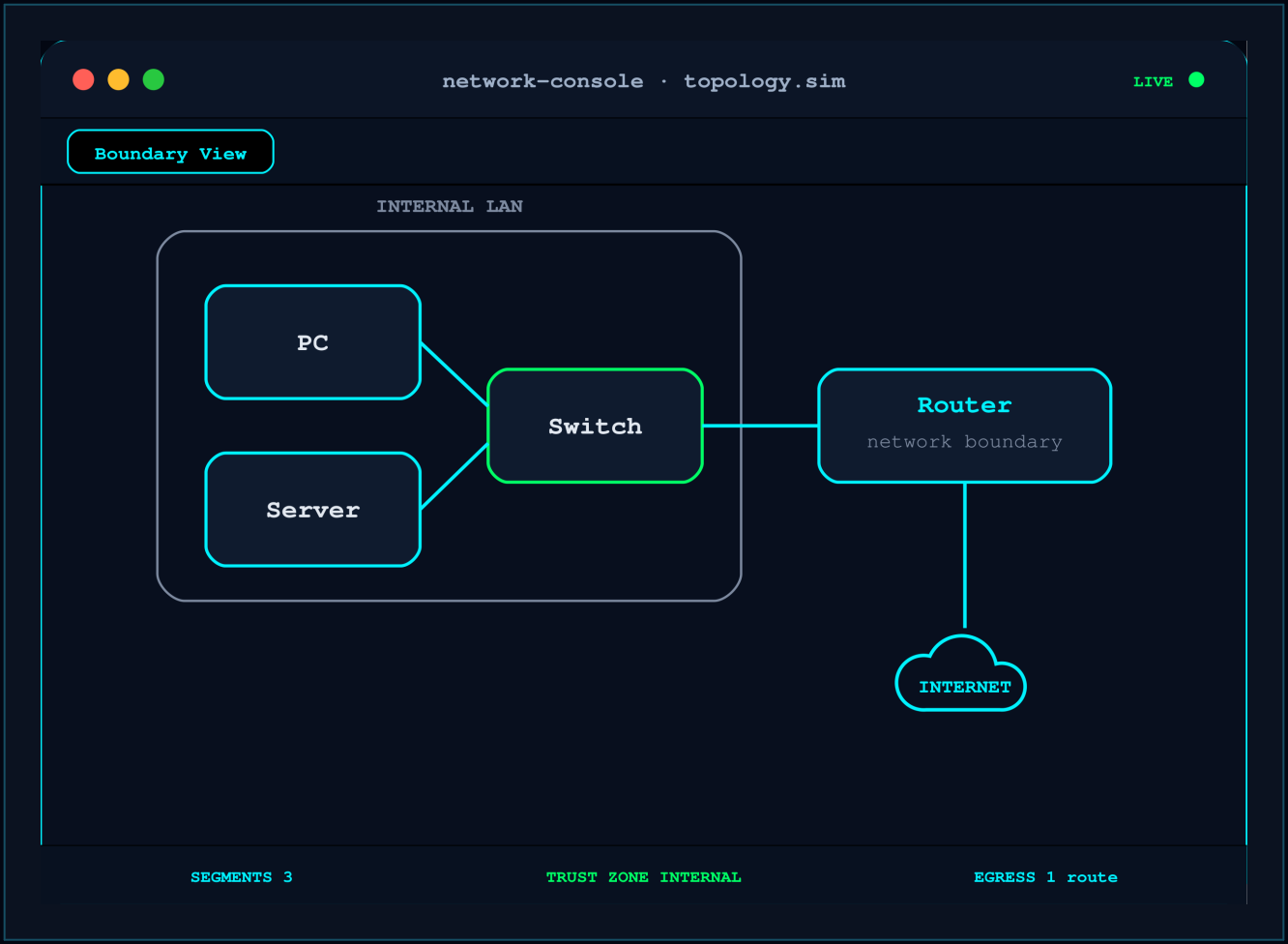
As part of my cybersecurity learning journey, I completed the **Extending Your Network** room on TryHackMe. The room brought together several networking concepts that are fundamental to understanding how systems communicate beyond a local network, and more importantly, how that communication can be controlled and secured.

Rather than treating port forwarding, firewalls, VPNs, routers, and switches as isolated topics, I approached the lab as a single security architecture. The central question became: **How does traffic move from one network to another, and where can we control or secure that traffic?**

Platform	TryHackMe
Room	Extending Your Network
Focus	Network Security & Networking Fundamentals
Areas Covered	Port Forwarding · Firewalls · VPNs · Routers · Switches · Network Simulation
Analyst	Nazline Mwita, Cybersecurity Assurance Lead, HarLyn Digital Partners

1. From LAN to the Internet: Understanding the Network Boundary

A Local Area Network (LAN) allows devices such as computers, servers, printers, and other systems to communicate within a defined network.



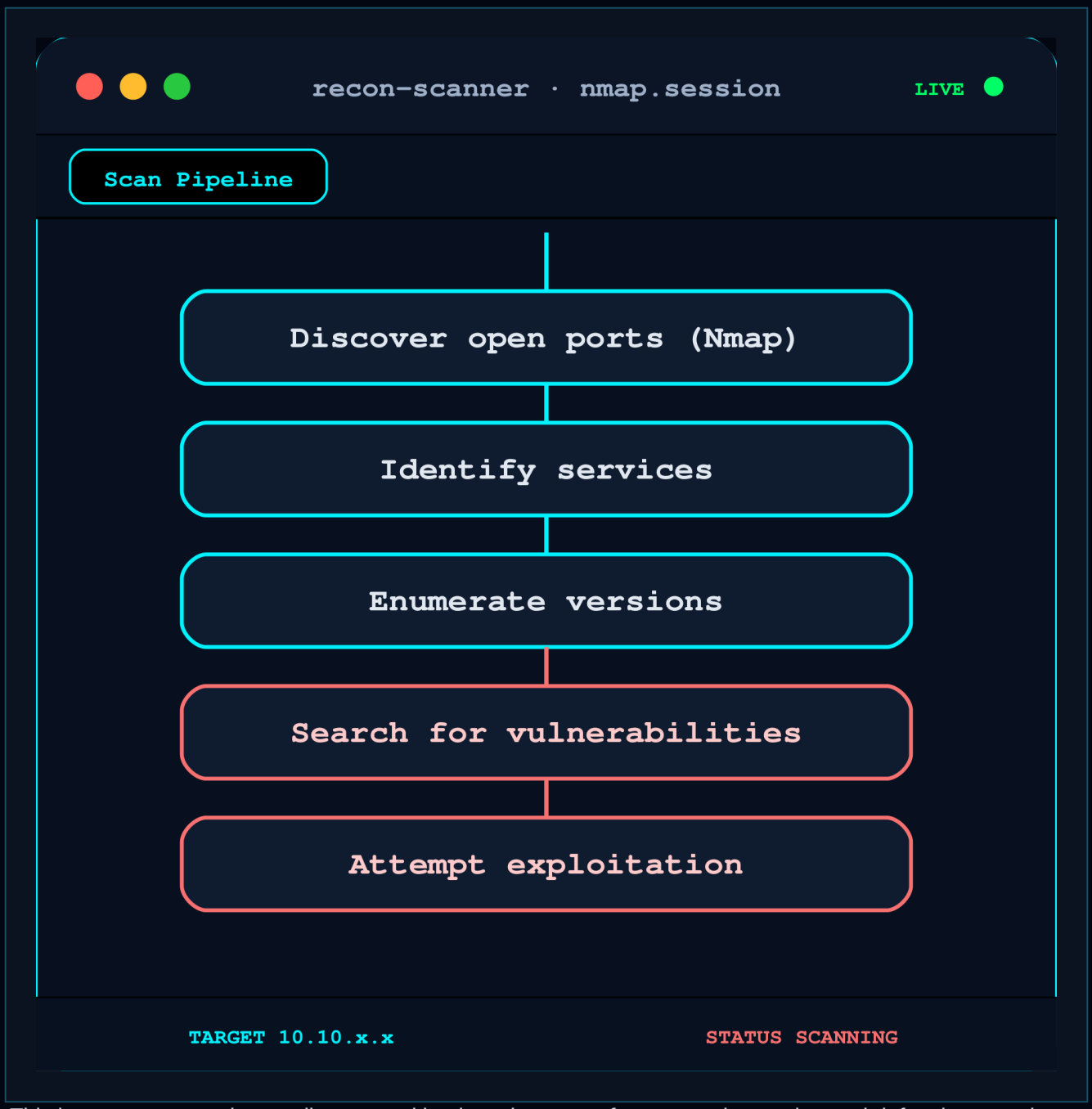
The router becomes an important boundary between the internal network and external networks. From a cybersecurity perspective, this boundary matters because systems inside a private network should not automatically become accessible from the Internet.

> **Security Principle**
>
> **Connectivity must be intentional.**

2. Port Forwarding: Making Internal Services Reachable

One of the first concepts explored was **port forwarding**. A service may be running internally on something like `192.168.1.10:80`, reachable from the internal network, but not from external users. Port forwarding allows a router to map an externally reachable address and port to an internal service.

The important lesson for cybersecurity is that **port forwarding increases exposure**. Opening a port does not automatically mean the service is secure. If an administrator exposes `Public_IP:80` → `Internal_Web_Server:80`, that service becomes reachable from outside the network, and its security suddenly matters much more.



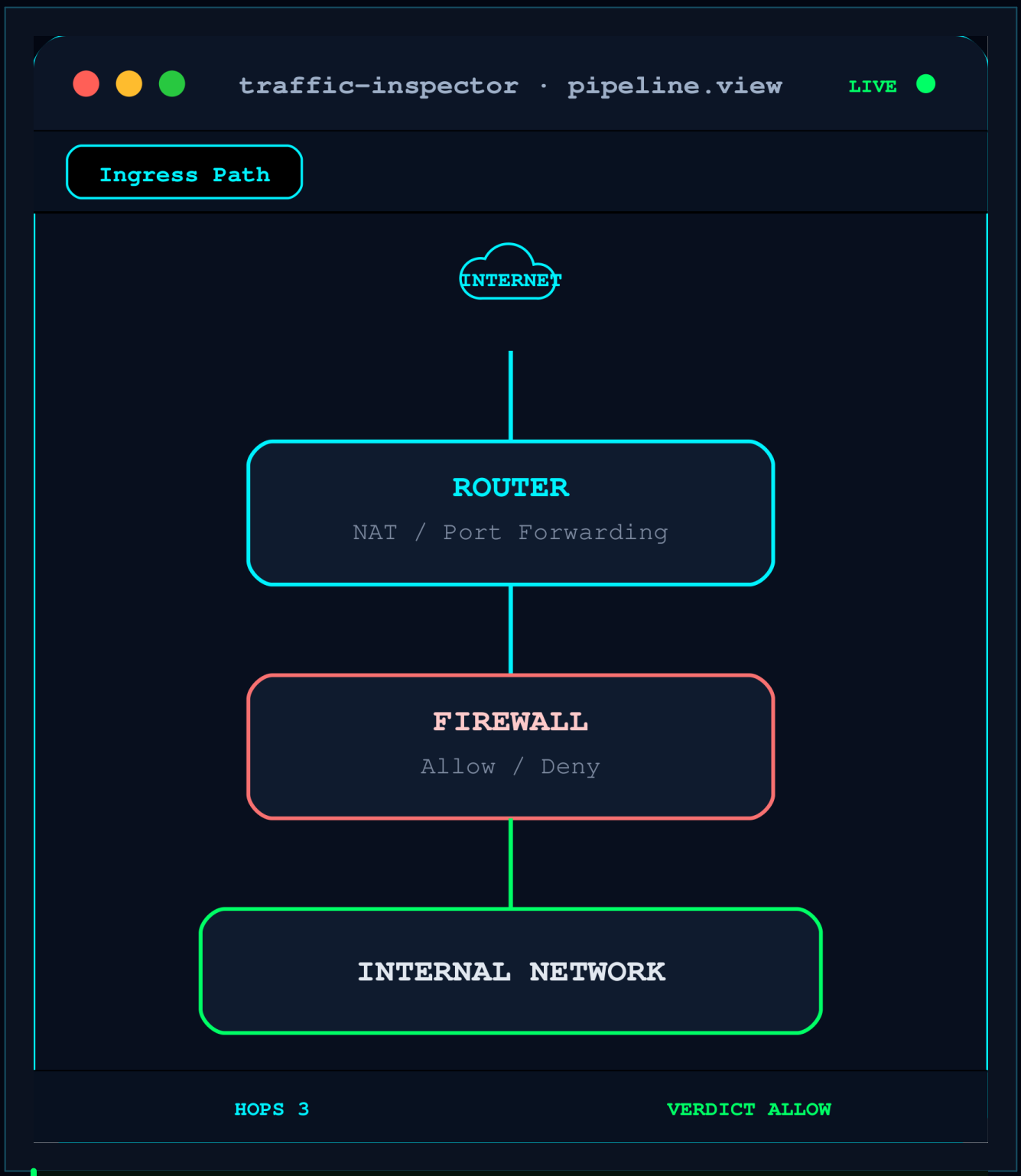
This is one reason understanding networking is so important for penetration testing and defensive security.

3. Port Forwarding ≠ Firewall

One of the most important distinctions from this lab was the difference between **port forwarding and firewall filtering**. They solve different problems.

Port forwarding determines where traffic should be sent.

Firewall determines whether traffic should be allowed or blocked according to security rules.



Security Perspective

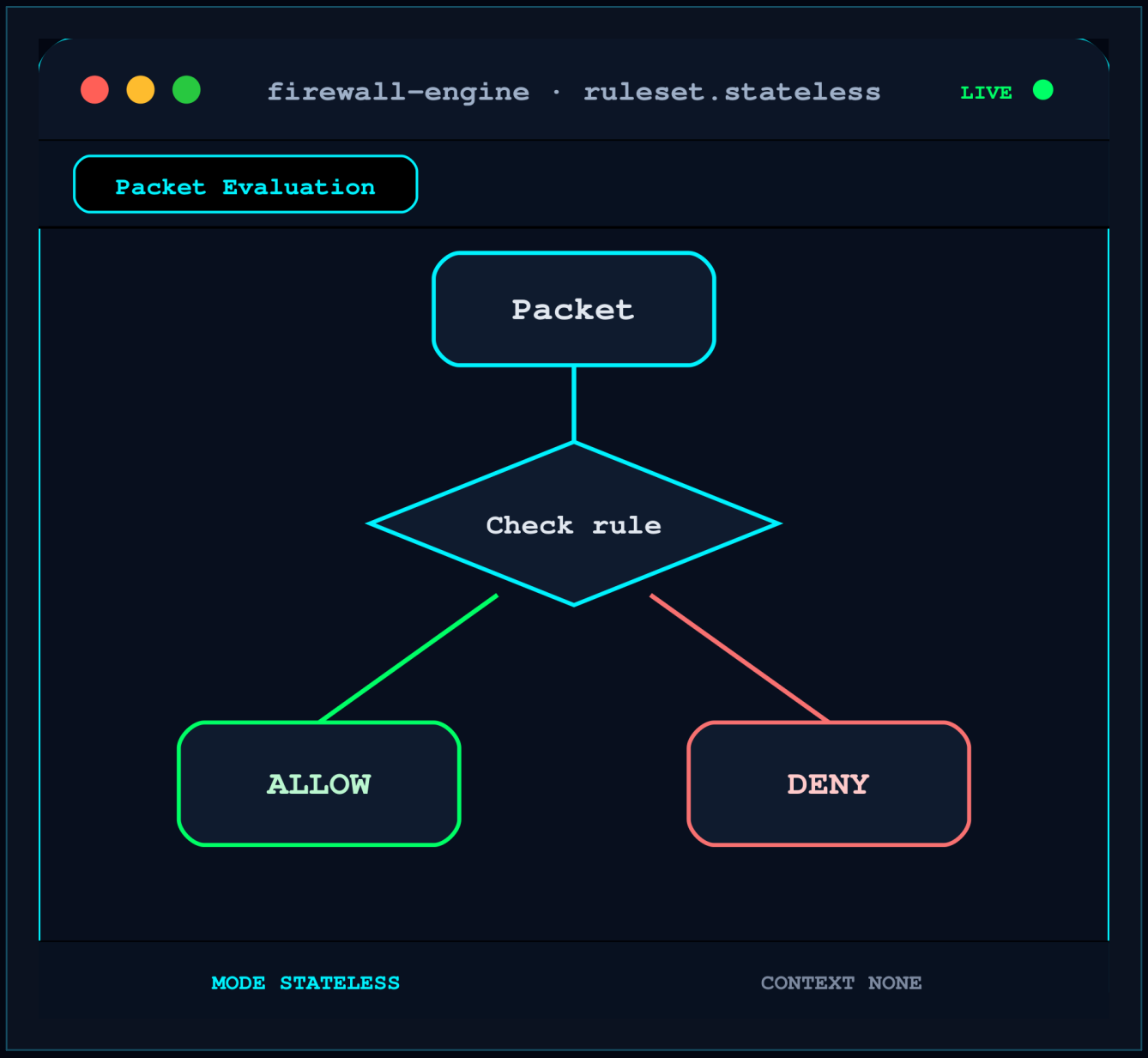
A reachable service should not automatically be a trusted service.

4. Firewalls: Controlling Network Traffic

Firewalls act as security control points between networks or security zones. They can inspect traffic and apply rules based on characteristics such as source IP, destination IP, source port, destination port, protocol, and connection state.

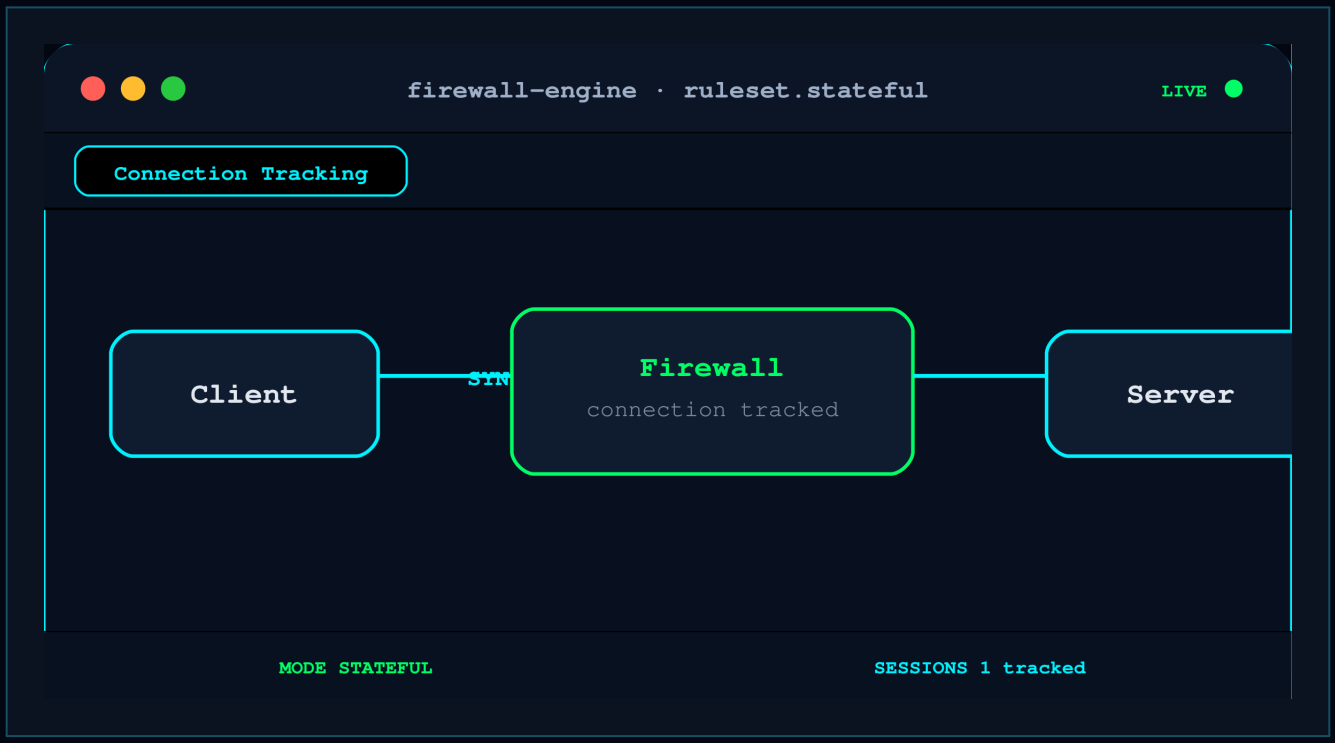
Stateless Firewalls

A stateless firewall evaluates packets individually against predefined rules. It does not maintain awareness of the complete connection.



Stateful Firewalls

A stateful firewall tracks the state of network connections, understanding whether traffic belongs to an established connection, giving it additional context for filtering decisions.

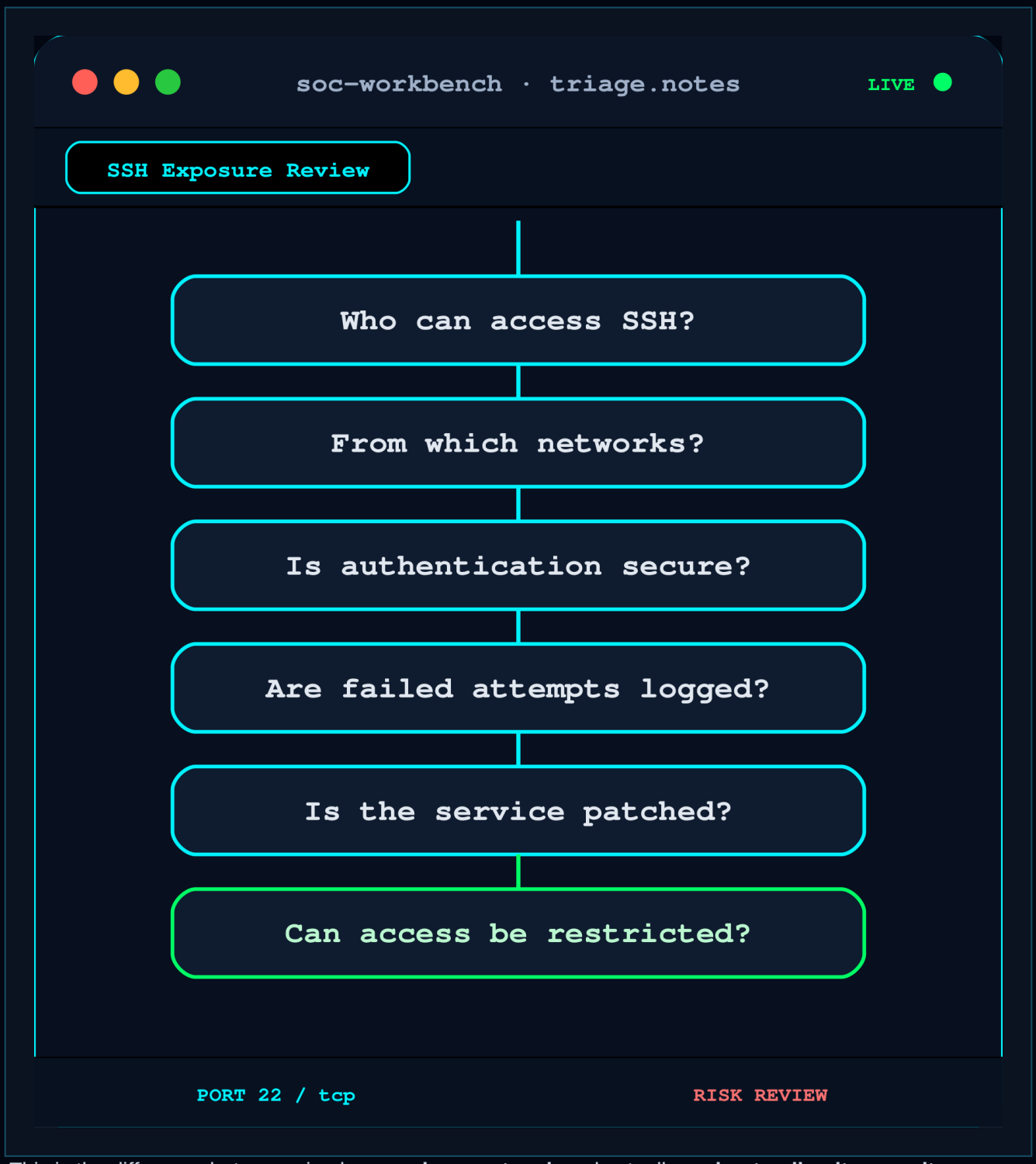


The room places these firewall concepts within the Layer 3 and Layer 4 portions of the OSI model.

5. Thinking Like a Security Analyst

Learning firewall rules changed how I think about network traffic. Instead of asking “Is this port open?” I should also ask “Why is this port open?”, “Who should be able to access it?”, and “What happens if this service is compromised?”

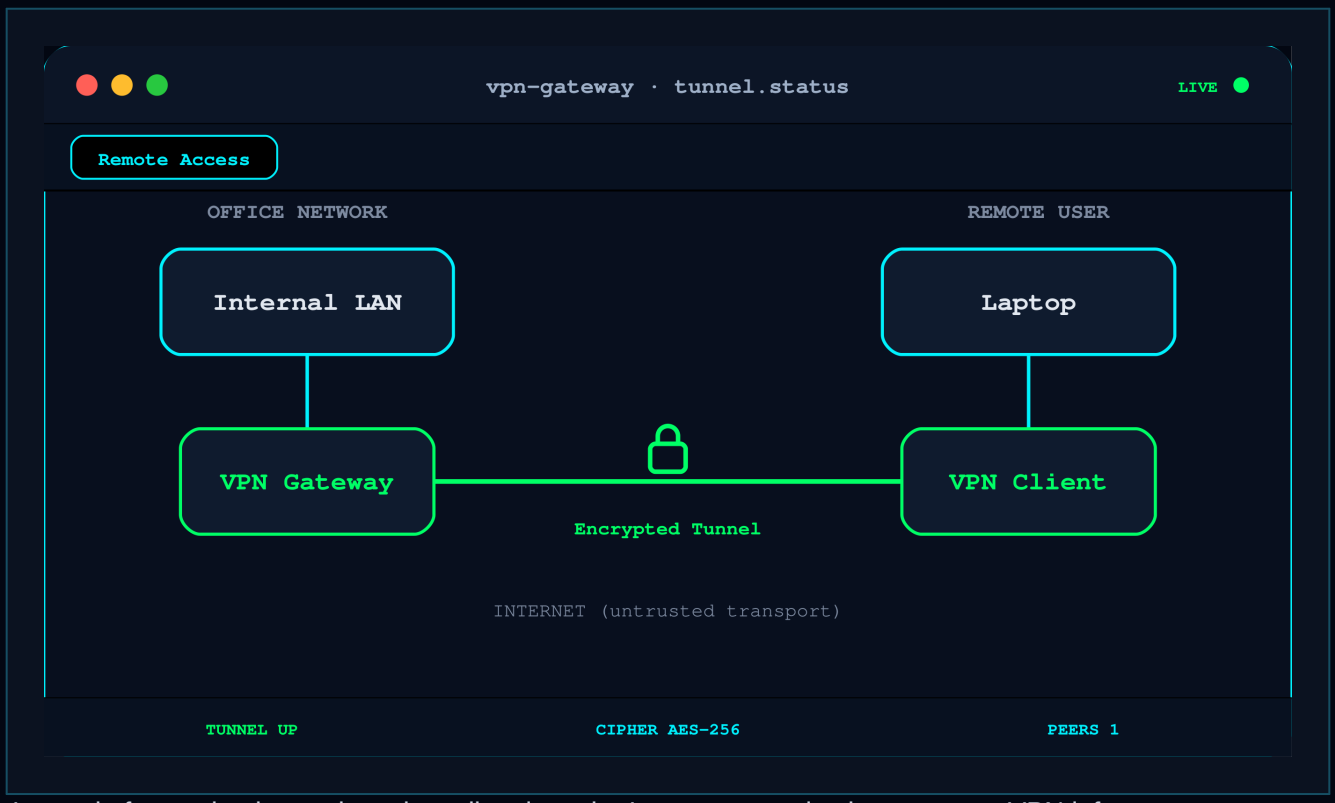
For example, SSH (port 22) being open does not automatically mean something is wrong. The real security questions become:



This is the difference between simply **scanning a network** and actually **understanding its security posture**.

6. VPNs: Extending a Private Network Securely

The next major concept was the **Virtual Private Network (VPN)**: a protected communication channel across an otherwise untrusted network.



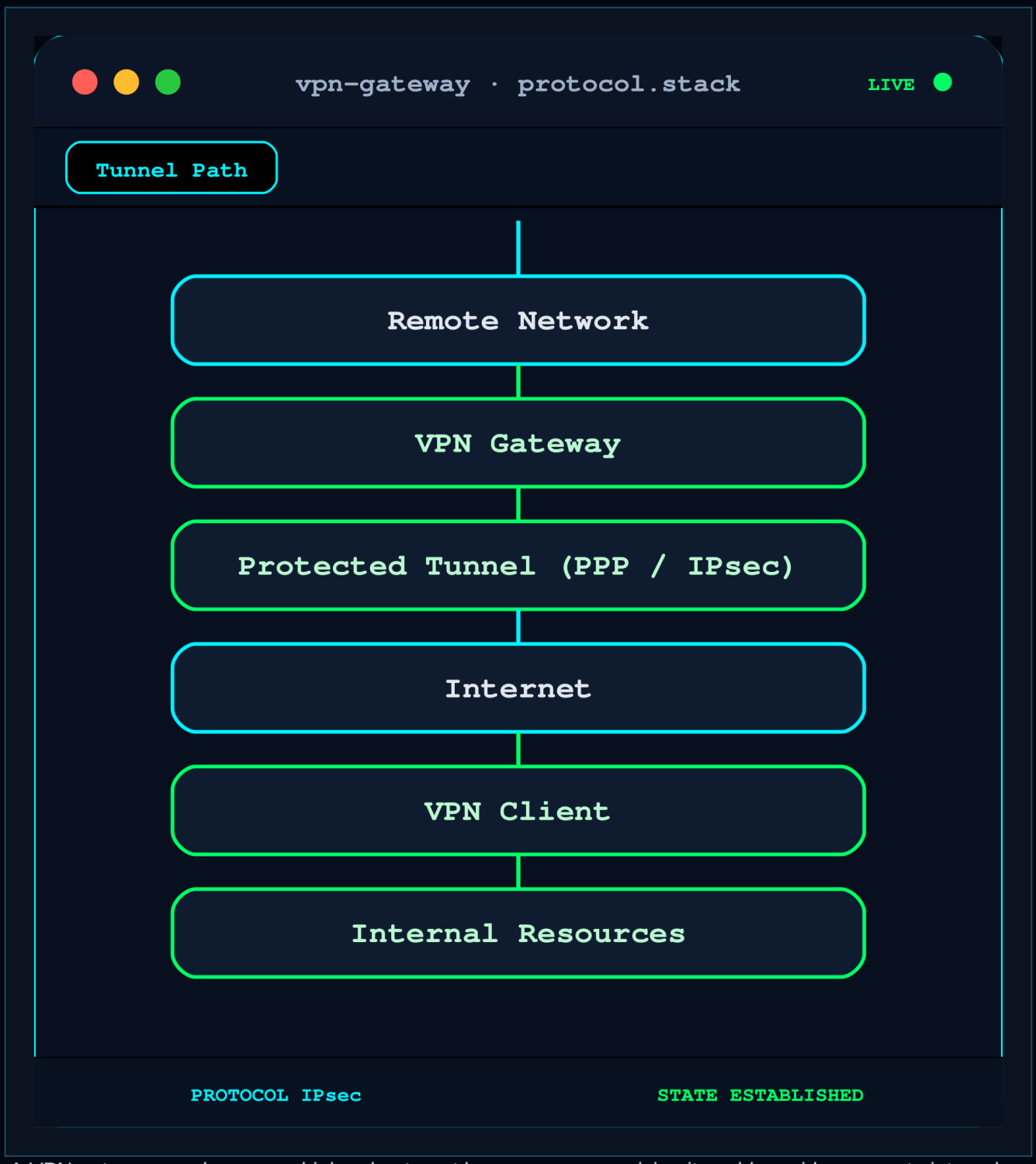
Instead of exposing internal services directly to the Internet, organizations can use VPN infrastructure to provide controlled remote access.

> **Security Advantage**
>
> The Internet becomes the transport medium without necessarily becoming the trusted network.

TryHackMe itself uses OpenVPN to provide access to its intentionally vulnerable training machines, demonstrating the practical role of VPNs in creating controlled connectivity between environments.

7. VPN Technologies and Security

The lab also introduced technologies associated with VPN communication, including **PPP** and **IPsec**. The important takeaway was not memorizing the technologies, but understanding the bigger concept:



A VPN gateway can become a high-value target because compromising it could provide access to internal resources. VPN security therefore involves more than encryption. It also involves:

- Strong authentication
- Access control
- Patch management

- Logging
- Monitoring
- Network segmentation
- Least privilege

8. LAN Networking Devices: Understanding the Infrastructure

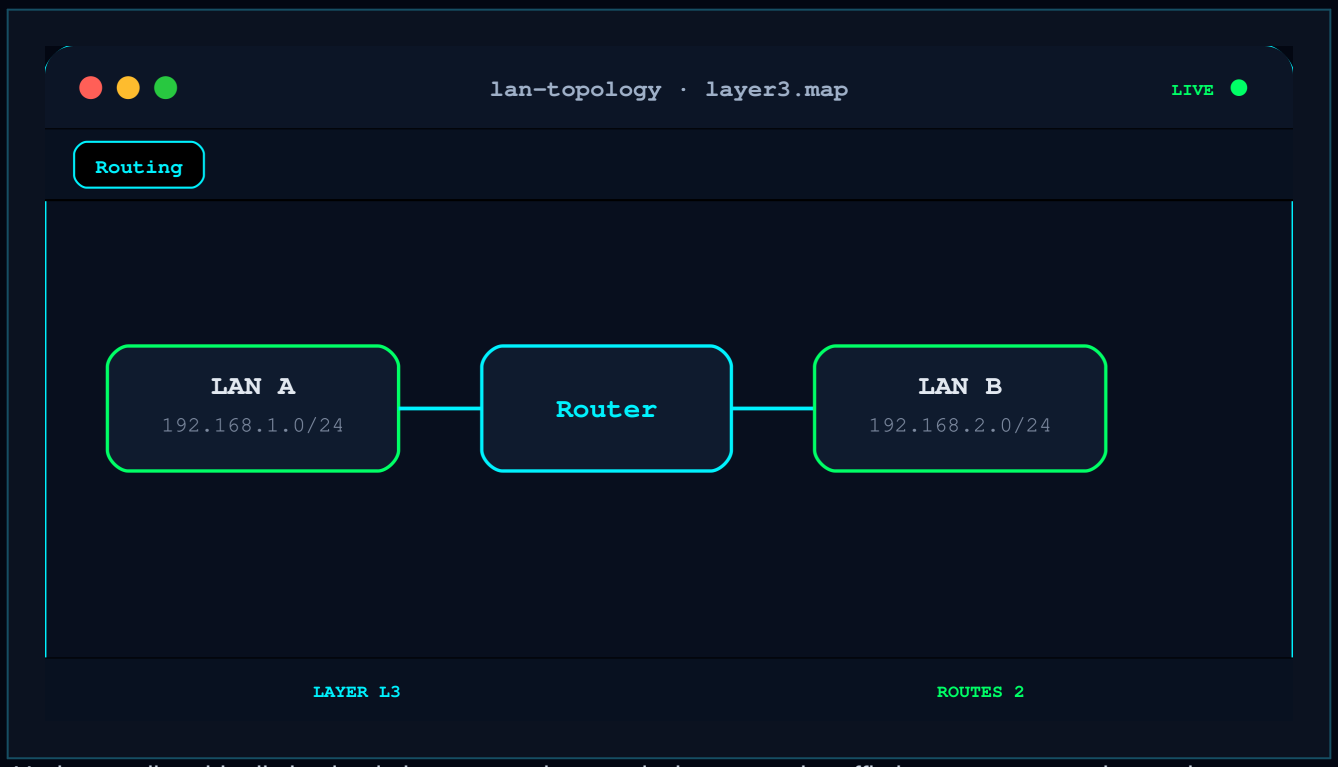
Switches

Switches primarily connect devices within a network.

Layer 2 switches primarily operate using Ethernet/MAC addressing. Layer 3 switches can also perform routing functions.

Routers

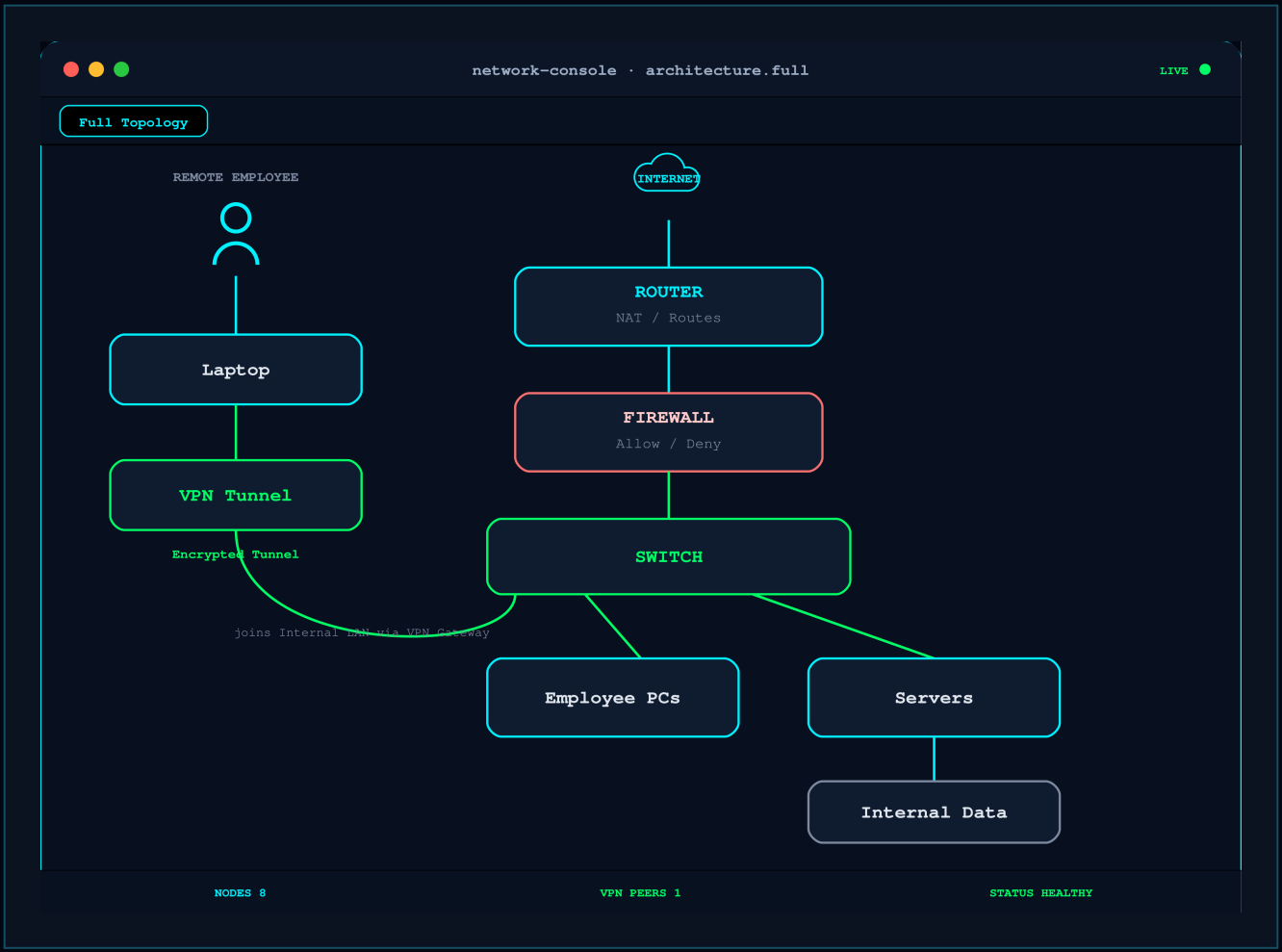
Routers connect different networks. Their fundamental job is **routing**: determining where packets should go next.



Understanding this distinction is important when analysing network traffic because an attacker and a target may not necessarily exist on the same network segment.

9. Putting Everything Together

The biggest value of this lab was seeing how all these components interact within one small company network architecture:



Router → connects networks and performs routing/NAT functions.

Port Forwarding → selectively exposes internal services externally.

Firewall → controls which traffic is permitted.

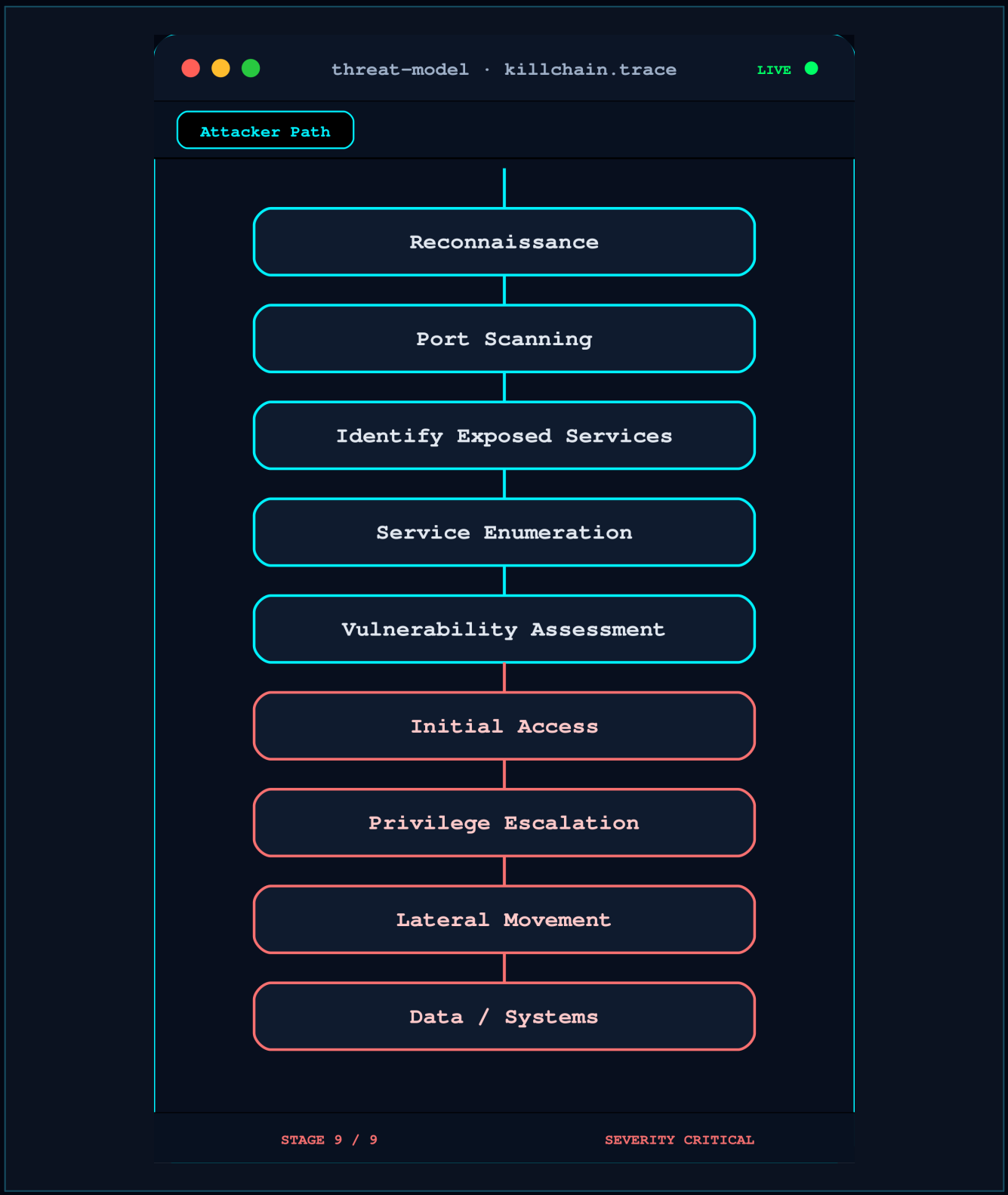
VPN → provides protected remote connectivity.

Switch → connects devices within LAN segments.

Servers → provide business services that must be protected.

10. The Attacker's Perspective

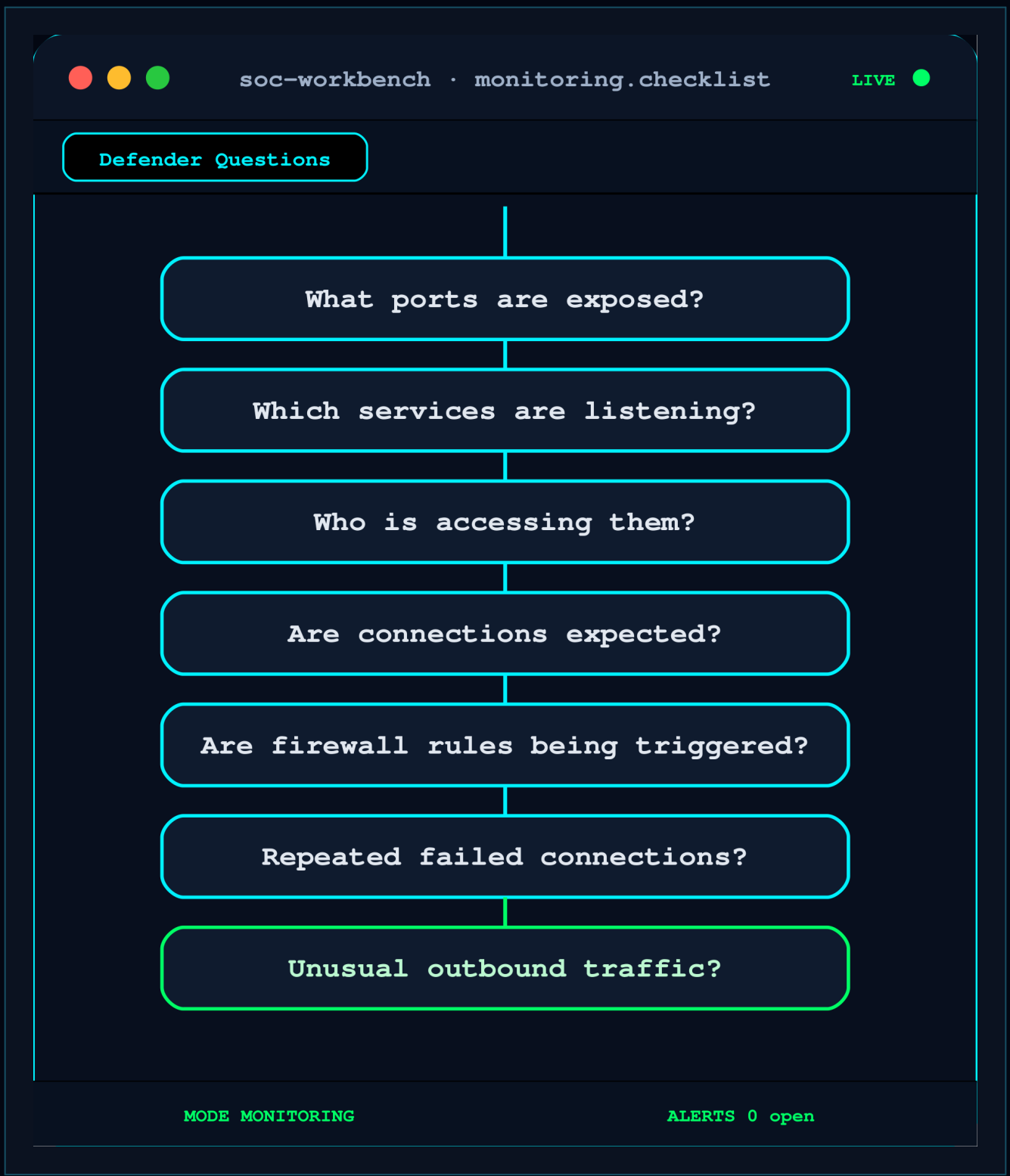
Understanding the network from a defensive perspective also means understanding what an attacker may see. A simplified attack path:



This is why network fundamentals are directly connected to penetration testing, SOC operations, incident response, and network defense. If I do not understand how traffic is supposed to move through a network, it becomes much harder to recognize when that traffic is abnormal.

11. The Defender's Perspective

From the defensive side, the same architecture becomes a monitoring opportunity. A security analyst can ask:



This connects networking directly to **SOC and security monitoring**. Repeated connection attempts against many ports could indicate reconnaissance. Unexpected remote access through a VPN account could require investigation. Unexpected outbound connections from an internal server could indicate compromise or data exfiltration.

Modern Network Security

Depends not only on preventing traffic, but also on understanding and monitoring traffic.

12. Practical Takeaways

After completing this lab, I can connect several networking concepts that previously might have seemed independent:

Concept	Security Relevance
Port Forwarding	Controls external access to internal services
NAT	Translates between network addressing contexts
Firewalls	Enforce traffic-control policies
Stateful Filtering	Adds connection-state awareness
Stateless Filtering	Evaluates packets individually
VPNs	Provide protected remote connectivity
Routers	Connect and route between networks
Layer 2 Switches	Connect devices within LANs
Layer 3 Switches	Provide switching plus routing capabilities
Network Simulation	Helps visualize packet flow and communication

13. What This Means for My Cybersecurity Journey

This lab reinforced something important about becoming a cybersecurity professional: **Cybersecurity does not begin with exploitation. It begins with understanding how the system is supposed to work.**

Before identifying a vulnerability, I need to understand:

- What networks exist?
- Which systems communicate?
- Which ports are exposed?
- Which services should be reachable?
- Where are the trust boundaries?
- What traffic should be allowed?
- What traffic should be blocked?
- How is remote access provided?
- What would suspicious traffic look like?

Once I understand the intended architecture, abnormal behaviour becomes easier to recognize. That foundation supports the areas I am continuing to develop in cybersecurity, including **penetration testing, network security, SOC operations, vulnerability assessment, and incident response**.

Final Reflection

The most valuable lesson from **Extending Your Network** was not a single command or definition. It was learning to see a network as a collection of **communication paths and security boundaries**.

A router determines where traffic goes.

A switch connects devices.

Port forwarding determines which internal services can be reached externally.

A firewall determines which traffic should be permitted.

A VPN creates controlled remote connectivity.

And security professionals must understand how all of these components interact. That is the perspective I want to continue developing as I move deeper into cybersecurity:

> **Guiding Principle**
>
> **Understand the architecture. Understand the traffic. Understand the attack surface. Then secure it.**

Skills Demonstrated

Networking · Network Security · Port Forwarding · Firewalls · VPN · Routing · LAN · TCP/IP · OSI Model · Security Fundamentals · Traffic Analysis · Cybersecurity

Nazline Mwita, CompTIA Security+ certified Cybersecurity Assurance Lead and Co-Founder at HarLyn Digital Partners. Specializing in authorized web & API security assessments, KDPA compliance reviews, and defensive cloud architecture in Nairobi, Kenya.