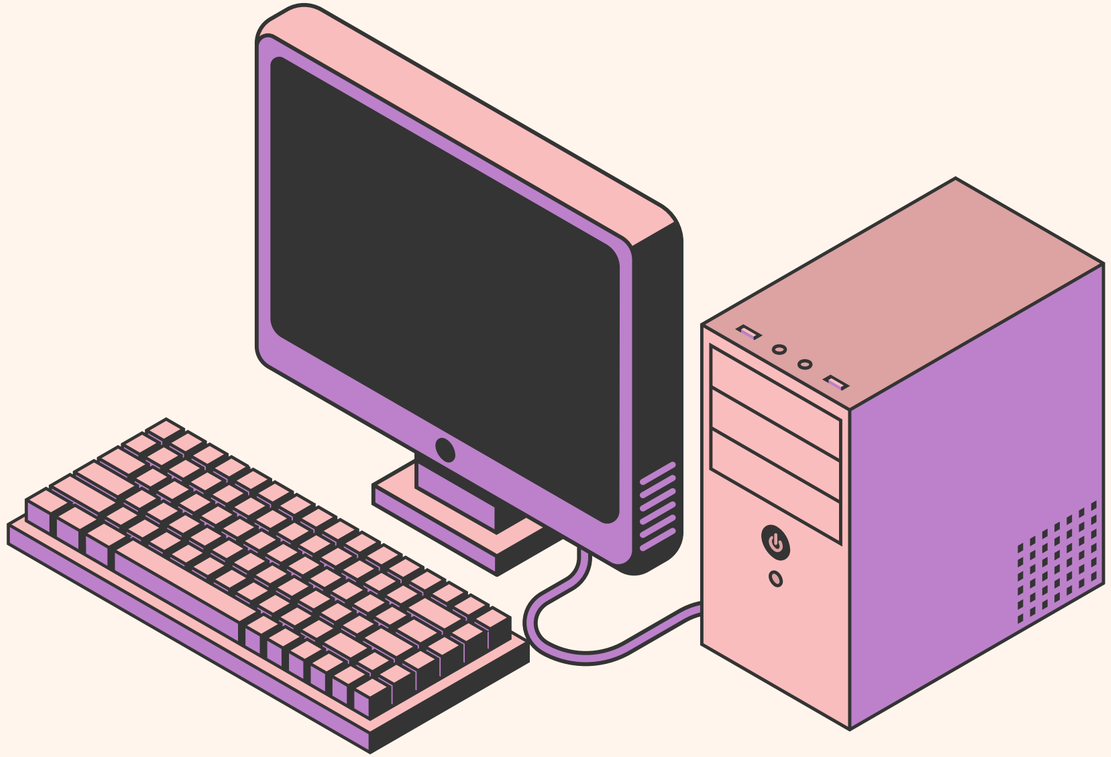
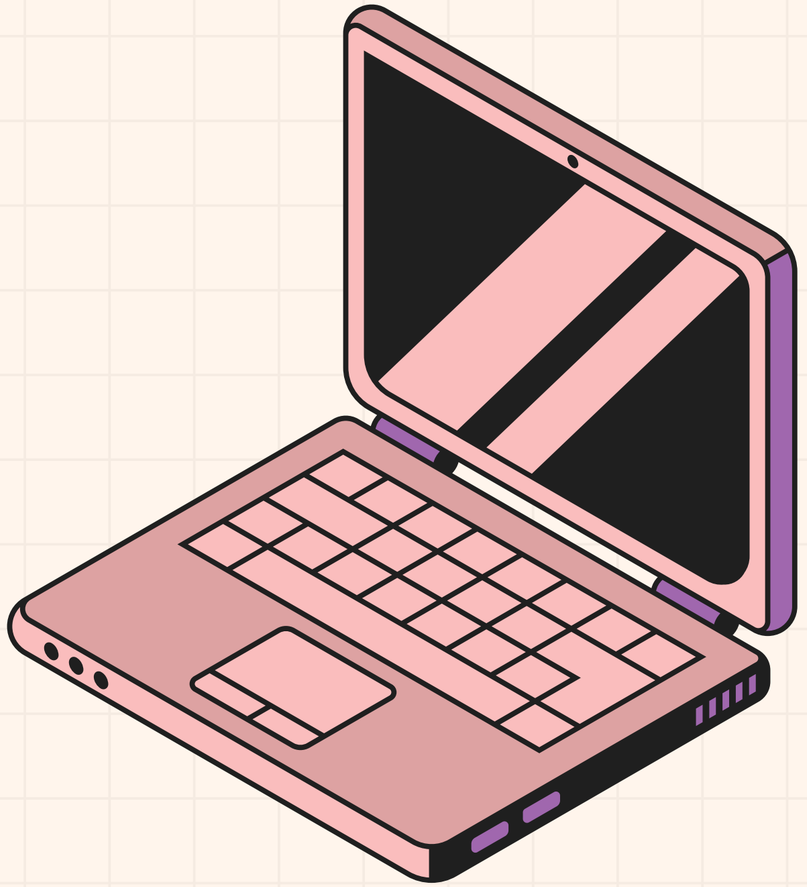
Implementing VPN Solutions with FortiGate



GOAL OF THE PROJECT

To design and simulate a secure Enterprise VPN architecture using GNS3 and FortiGate, covering:

- Basic LAN/WAN setup
- IPsec site-to-site VPN (HQ ↔ Branch)
- SSL-VPN remote access
- SD-WAN for intelligent WAN routing and failover



LAB TOPOLOGY

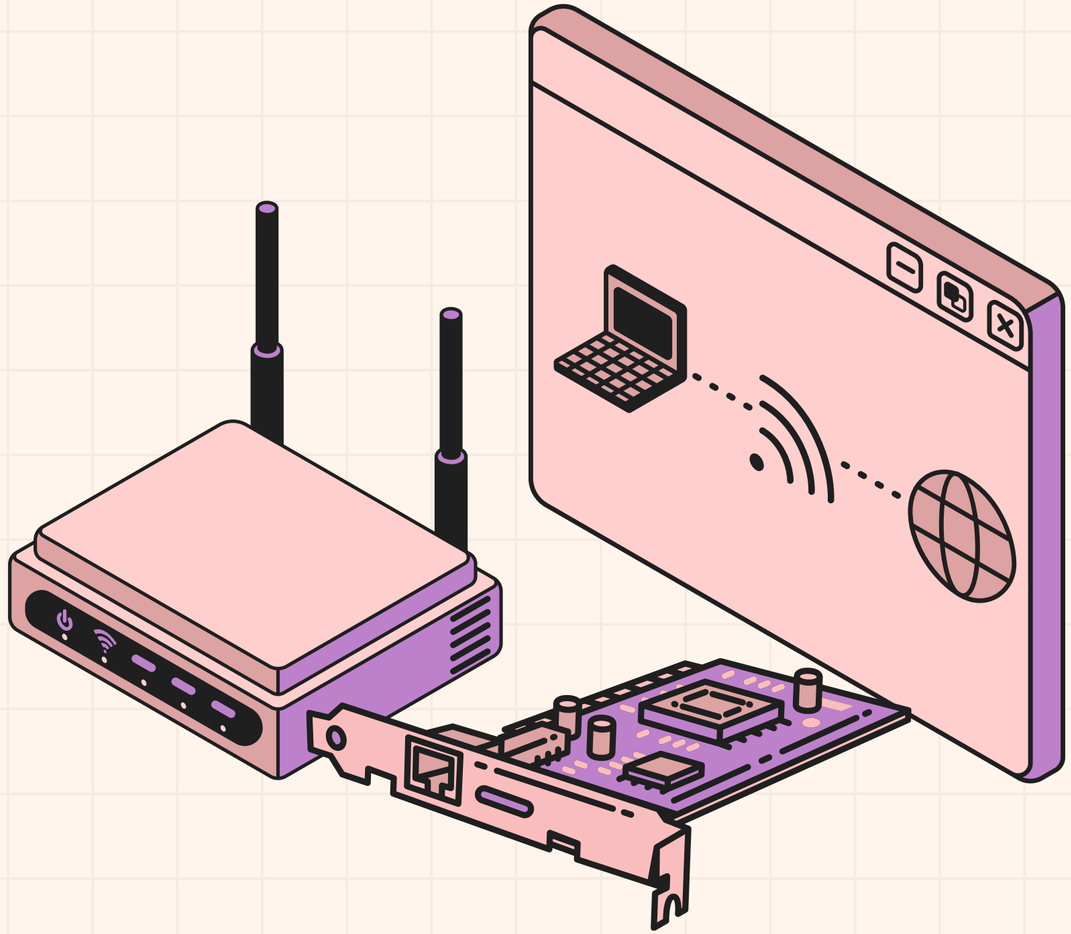
Components:

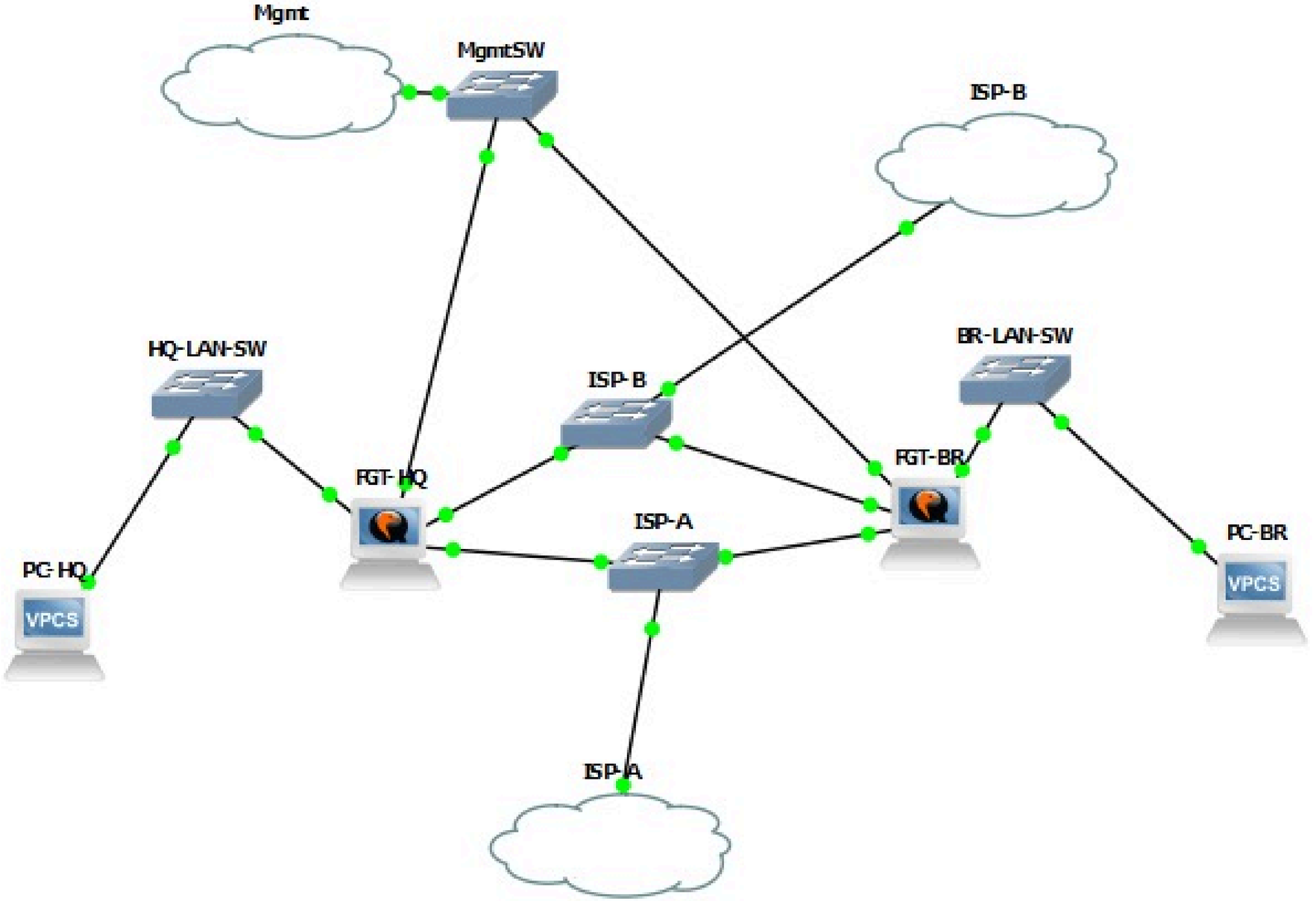
- 2 FortiGates (HQ & Branch)
- 2 “ISP clouds” simulating WAN networks
- HQ LAN + Branch LAN PCs
- Management network (VMnet1) for GUI access
- WAN networks (VMnet2 & VMnet3)
- GNS3 VM to emulate FortiGate KVM appliances

Management IPs:

- HQ GUI: Management IPs:
- HQ GUI:
- Your PC: 172.16.1.1 (VMnet1)
- Branch GUI: Management IPs:
- HQ GUI:
- Your PC: 172.16.1.1 (VMnet1)

Your PC: 172.16.1.1 (VMnet1)




Mgmt
MgmtSW
ISP-B
HQ-LAN-SW
ISP-B
BR-LAN-SW
FGT-HQ
FGT-BR
ISP-A
PC-HQ
VPCS
PC-BR
VPCS
ISP-A

WHAT WE SUCCESSFULLY BUILT

1. LAN Configuration
   - HQ LAN: 10.0.1.0/24
   - Branch LAN: 10.0.2.0/24
   - PCs assigned:
     - HQ PC: 10.0.1.10 / gateway 10.0.1.1
     - Branch PC: 10.0.2.10 / gateway 10.0.2.1

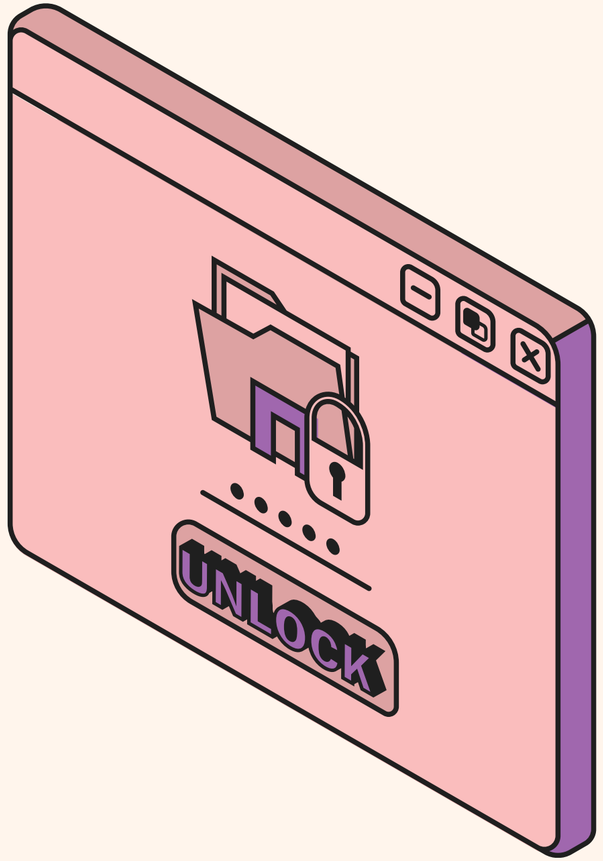
2. WAN Simulation

Using VMware VMnet networks:
   - WAN1 (ISP-A): 198.51.100.0/24
   - WAN2 (ISP-B): 203.0.113.0/24

Ping between WAN networks and PC worked perfectly.

3. IPsec VPN (HQ ↔ Branch)
   - Configured both Phase1 and Phase2
   - Tunnel successfully established using DES-SHA256 (limited by VM license)
   - HQ PC ↔ Branch PC communication worked through the tunnel

4. Management Network
   - Separate mgmt interface (port4)
   - Both FortiGates reachable via GUI
   - Admin port moved from 443 → 8443 to avoid conflict with SSL-VPN



WHAT WE COULD NOT COMPLETE

(because of FortiGate VM image limitations)
1.SSL-VPN
FortiClient failed with error (-5010): VPN server unreachable
Reason:

- The FortiGate image used was a limited/demo build, missing:
  - sslvpnd daemon
  - SSL-VPN debug commands
  - Listener on port 443
  - Full crypto support (AES missing)

Without the full VM license, SSL-VPN does not work.

2. SD-WAN
SD-WAN GUI did not show WAN interfaces (port2, port3).
Reason:

- SD-WAN feature is disabled in the limited/demo KVM image
- The image only showed mgmt interface as SD-WAN member
- Commands like config system virtual-wan-link partially worked but members never appeared

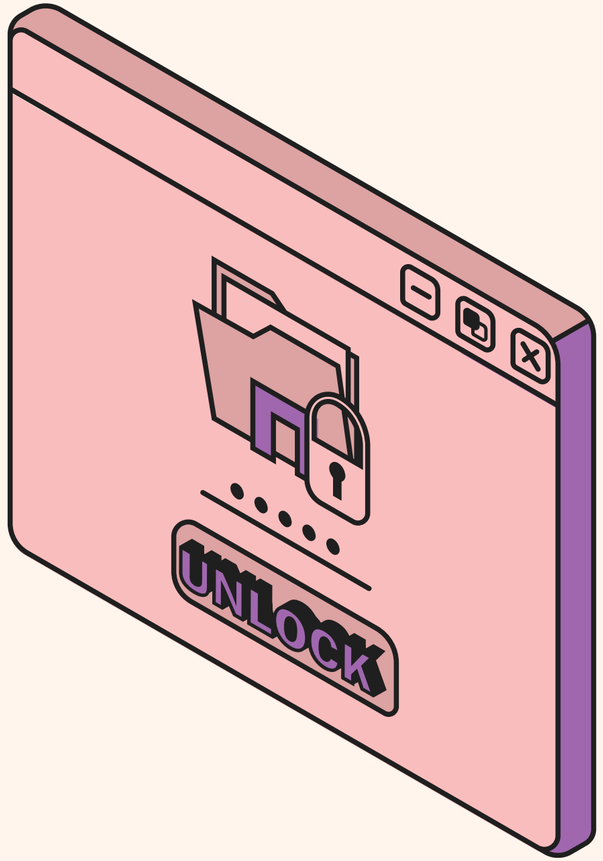
Conclusion:
SD-WAN requires the full-feature FortiGate VM image, not the minimal one.

3. Full Cryptography (AES)
IPsec proposals were limited to:

- DES-MD5
- DES-SHA1
- DES-SHA256

This is due to:

- Crypto restrictions in the demo/minimal FortiGate image
- No full license = no strong crypto

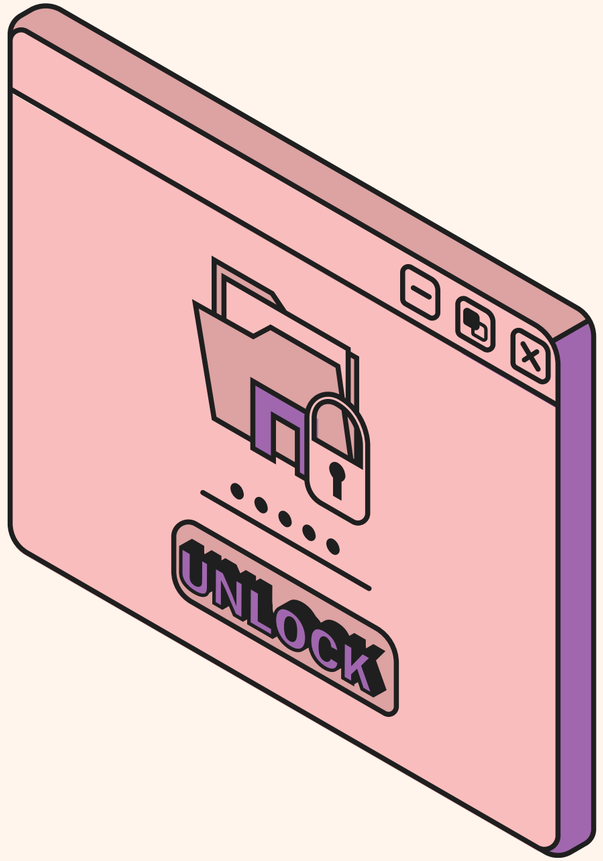


WHY THESE FEATURES FAILED

Because the downloaded qcow2 image was:

- A demo/minimal FortiGate KVM build
- Missing full feature modules:
  - SD-WAN
  - SSL-VPN
  - Advanced cryptography
  - Full CLI diagnostics
  - Listener processes
- Not an official licensed VM image

To enable all features, you must use the official Fortinet VM image:
FGT_VM64_KVM-v7.x.x-FORTINET.out.kvm.zip

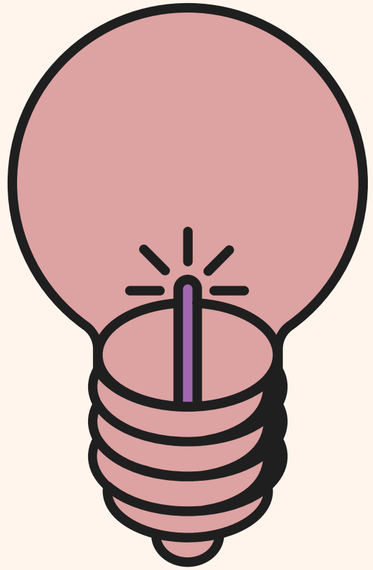


. WHAT WOULD WORK WITH THE FULL FORTIGATE VM LICENSE

Using the official VM image, we would be able to complete:

- Fully functional SSL-VPN
- Full SD-WAN configuration (WAN load balancing & failover)
- AES-256 IPsec tunnels
- Full diagnostic/debug commands
- FortiGate GUI features like:

SD-WAN monitoring
SSL-VPN portal
WAN link performance dashboards

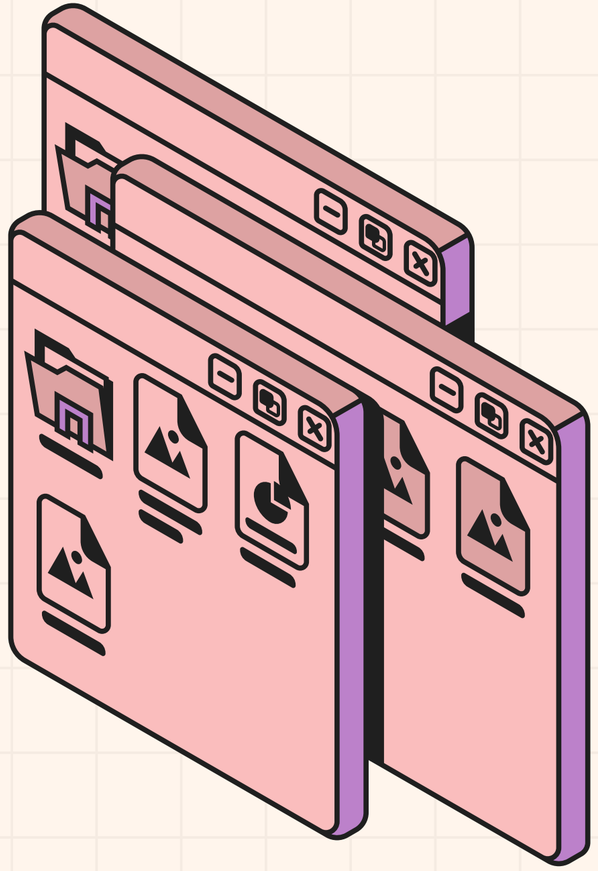


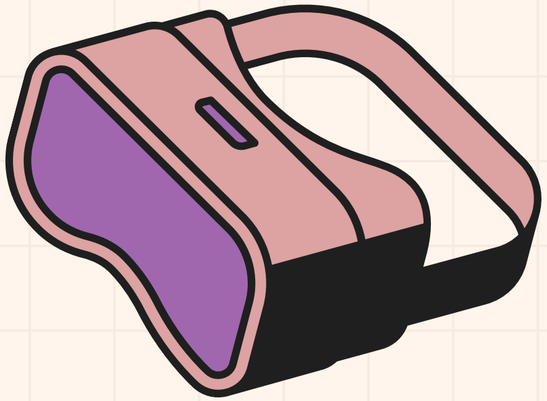
CONCLUSION

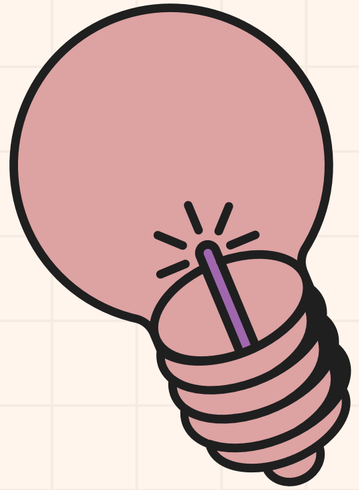
We successfully built the core VPN topology using GNS3 and FortiGate:
LAN environment
WAN simulation
Full IPsec tunnel HQ ↔ Branch
Management access & GUI functionality
But due to FortiGate VM license restrictions:

- SSL-VPN
- SD-WAN
- Advanced crypto

could not be completed.
With the official VM image, the entire project would run as designed.







THANK YOU