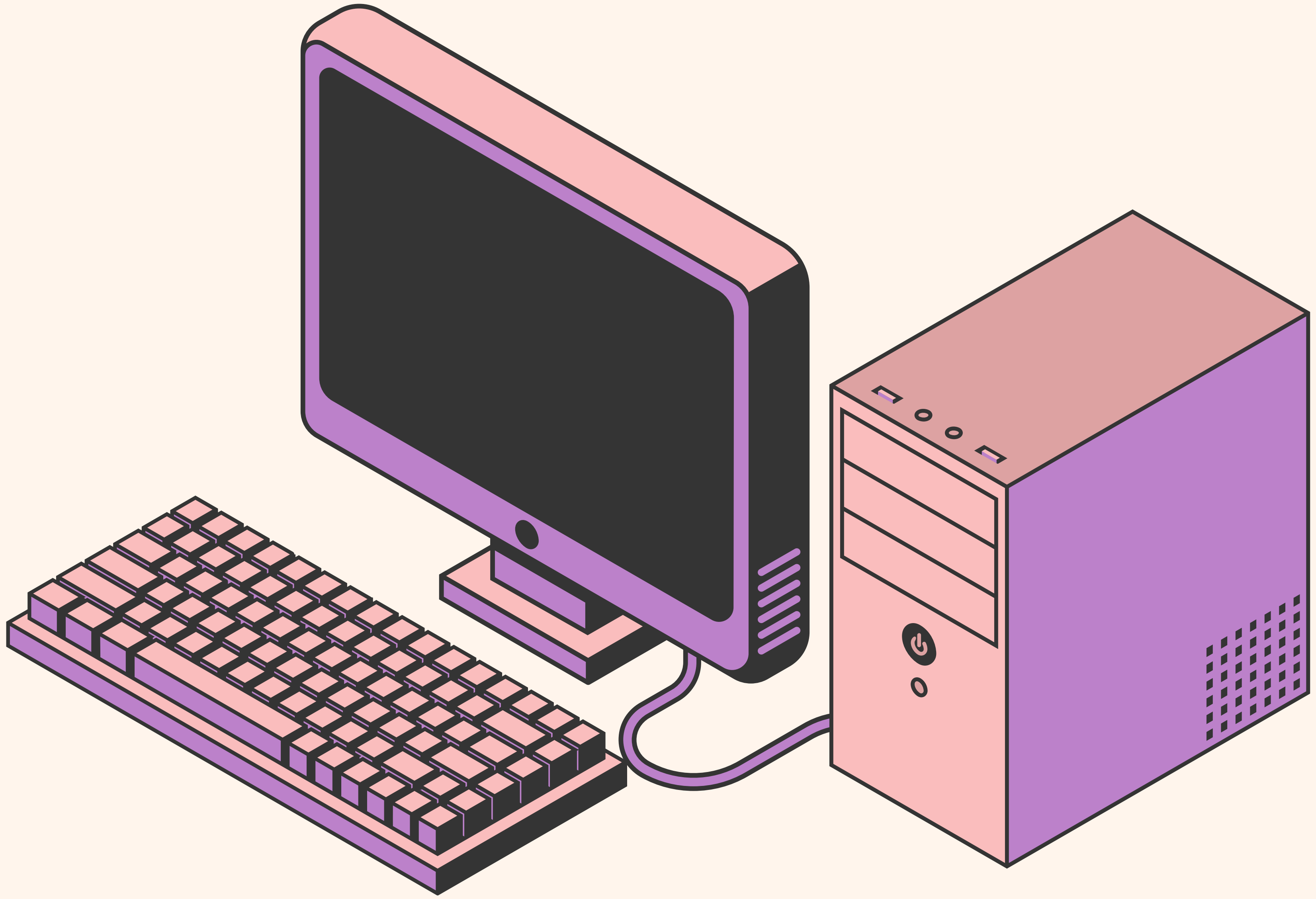
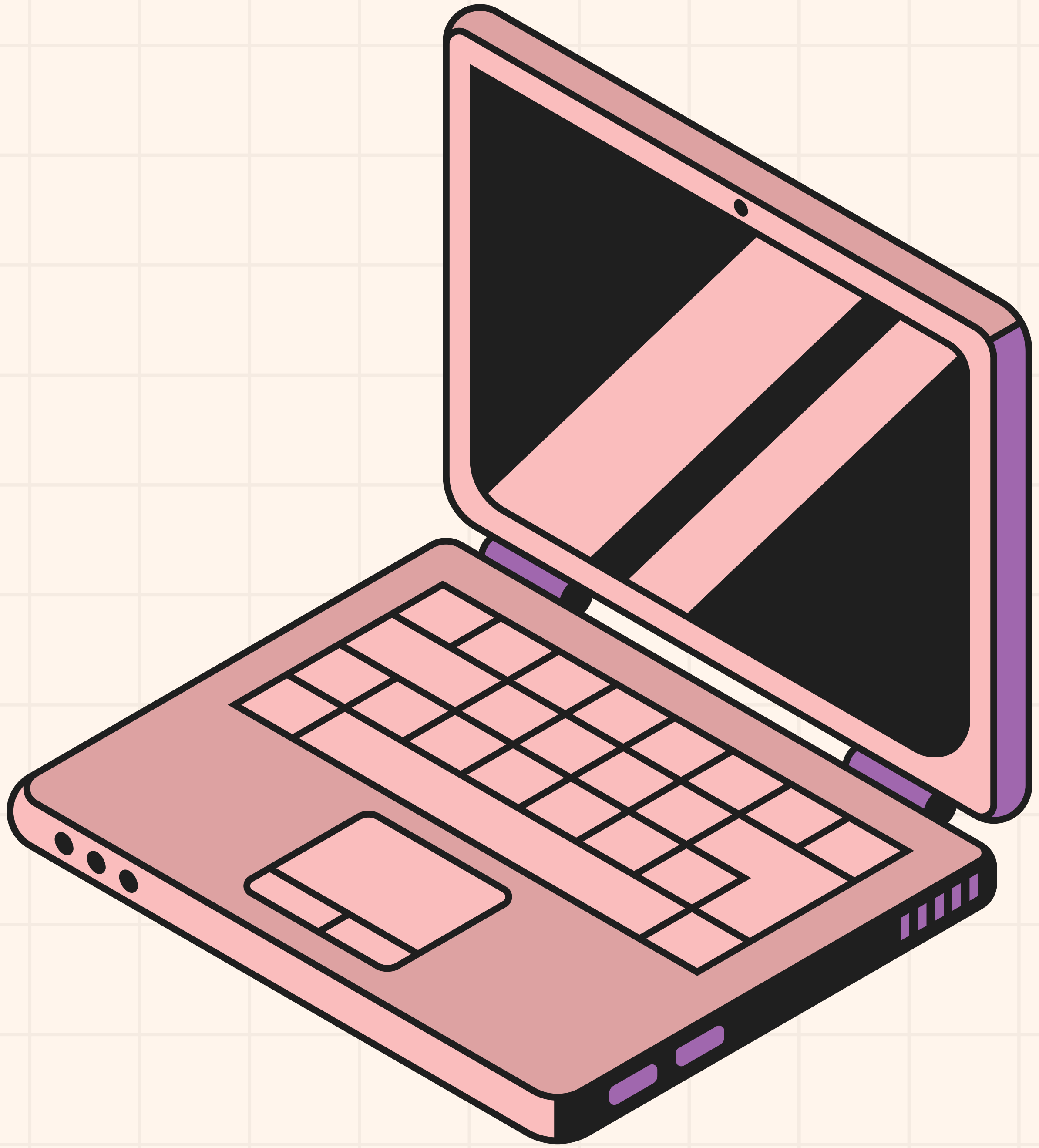
Implementing VPN Solutions with FortiGate



GOAL OF THE PROJECT

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

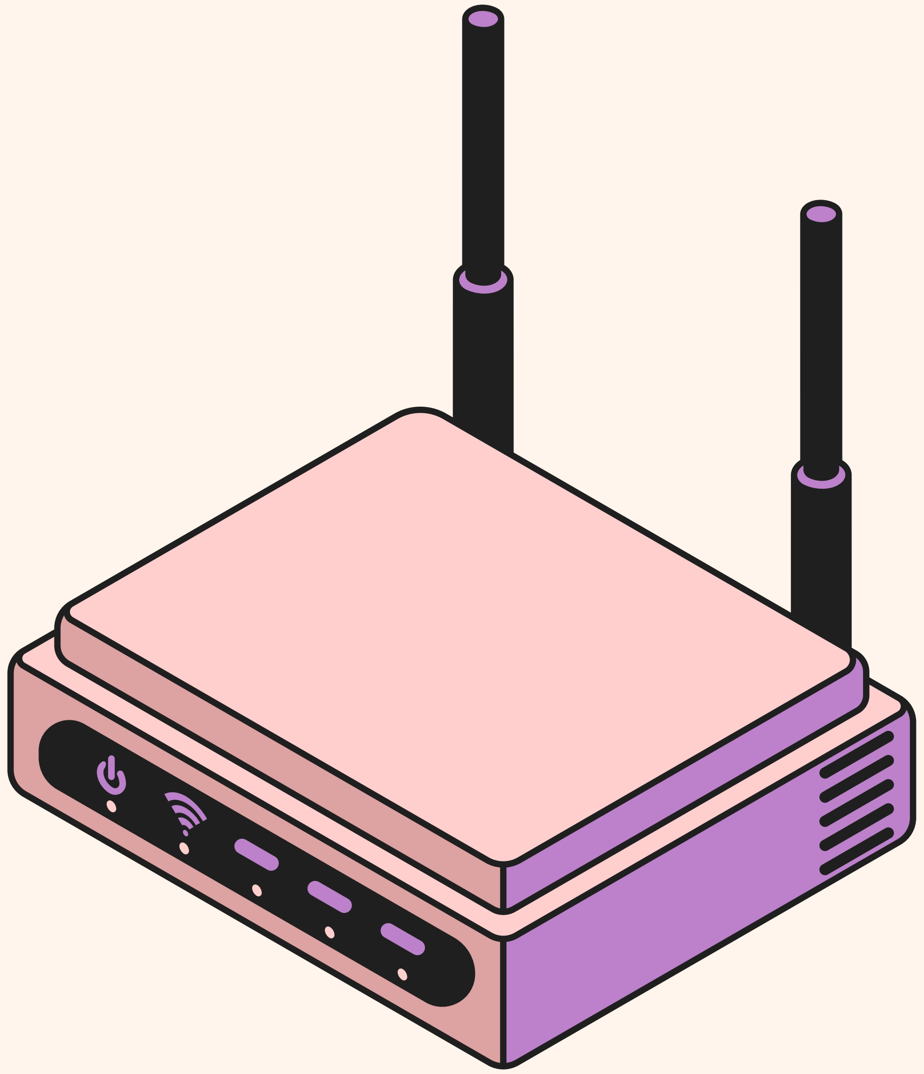
- Basic LAN/WAN setup
- IPsec site-to-site VPN (HQ ↔ Branch)
- SSL-VPN remote access
- SD-WAN for intelligent WAN routing and failover



What is VPN

In this project, the VPN (Virtual Private Network) is the secure communication tunnel that connects the HQ network and the Branch network over the simulated public WAN.

We implement a site to site Ipsec VPN That connects
Two different LANS and the traffic between these Two lans are encrypted

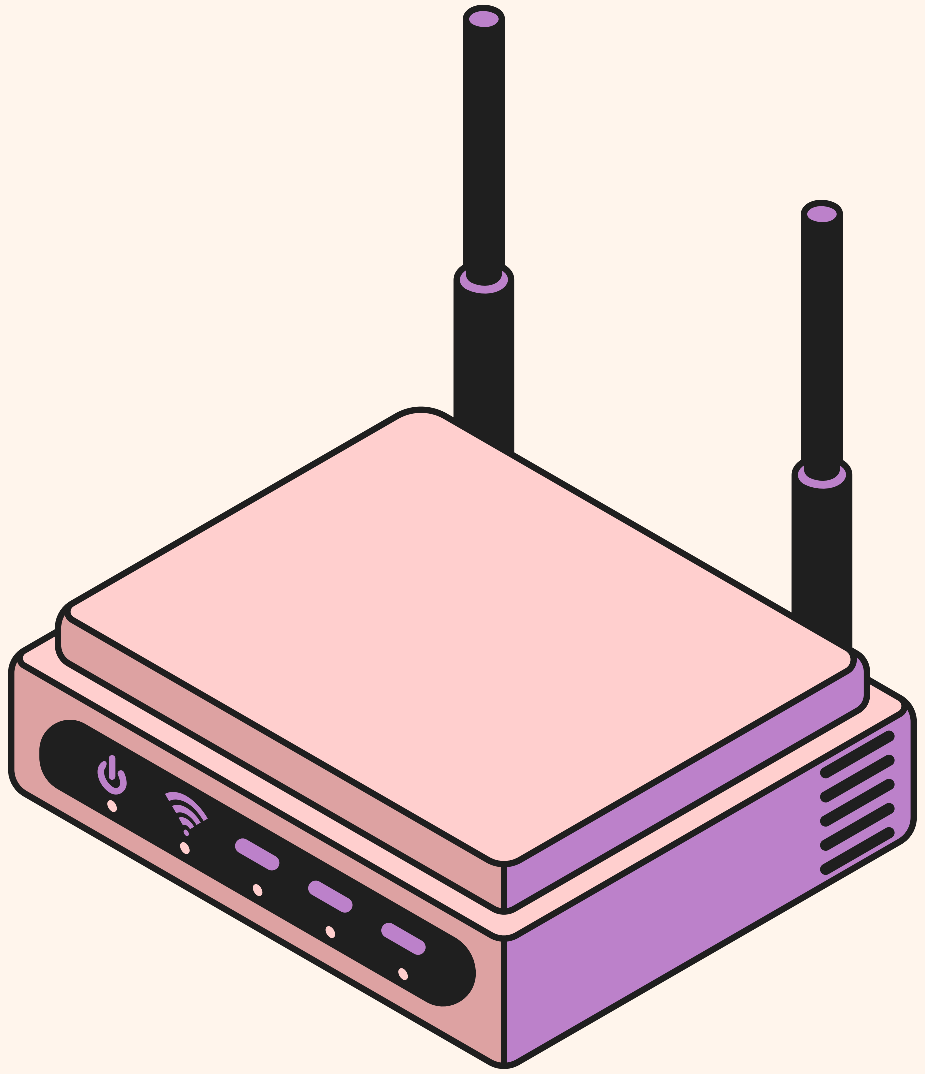


What is IPsec

IPsec is a set of protocols used to secure communication over untrusted networks

It creates a VPN tunnel that encrypts and protects data as it travels between two sites or devices.

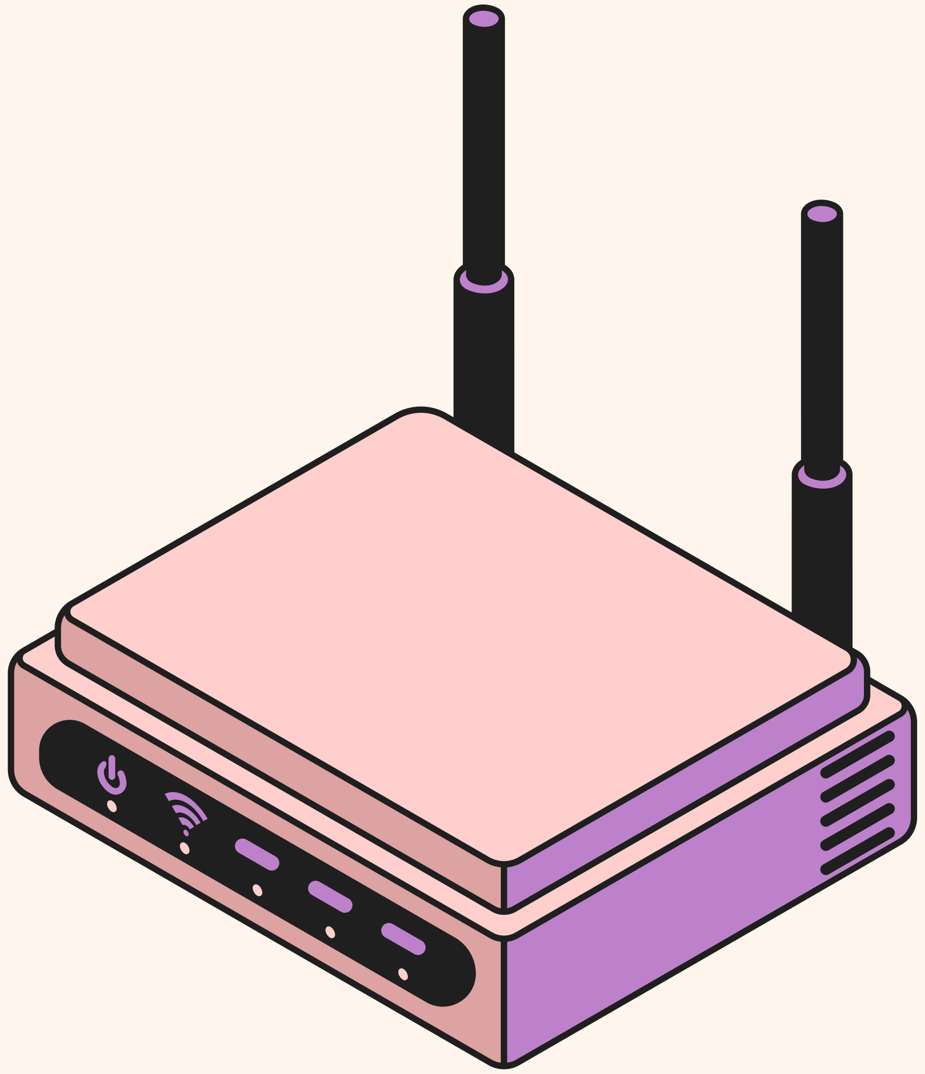
How it works
Using of trusted connection between HQ and branch by creating a secure tunnel between both sides



What is SSL

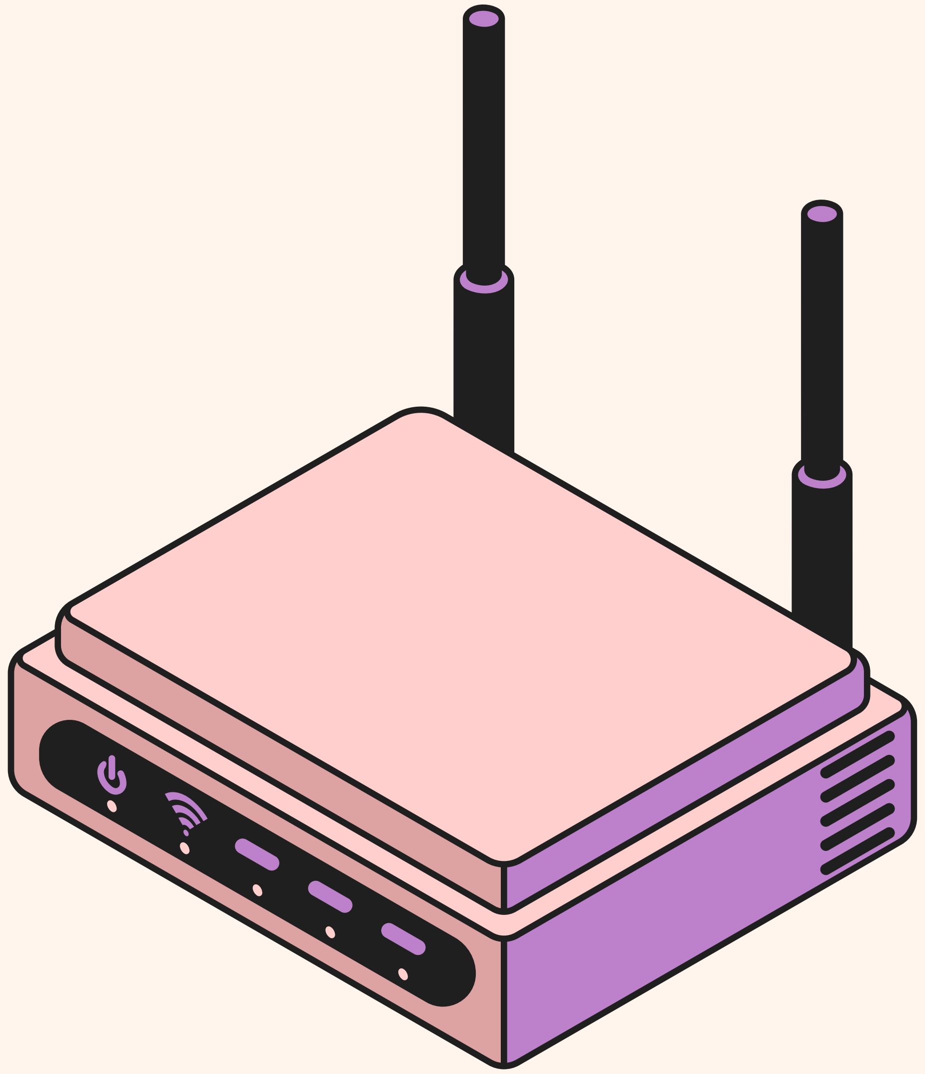
SSL is a protocol used to secure communication between a user and a server over the internet.
It encrypts the data being transmitted, ensuring confidentiality and protection from attackers.

How it works
When a remote user connects using SSL-VPN, the FortiGate creates a secure tunnel that protects the user's traffic and allows safe access to the internal network (HQ or Branch).



What is SD-WAN

SD-WAN improves WAN performance by dynamically selecting the best connection path for each type of traffic.
It uses real-time monitoring to optimize speed, reduce latency, and maintain reliability.



How it works
The firewall evaluates both WAN connections
(ISP-A and ISP-B). Based on latency, jitter, or packet loss, SD-WAN routes traffic through the best link and provides automatic failover if one ISP has issues.

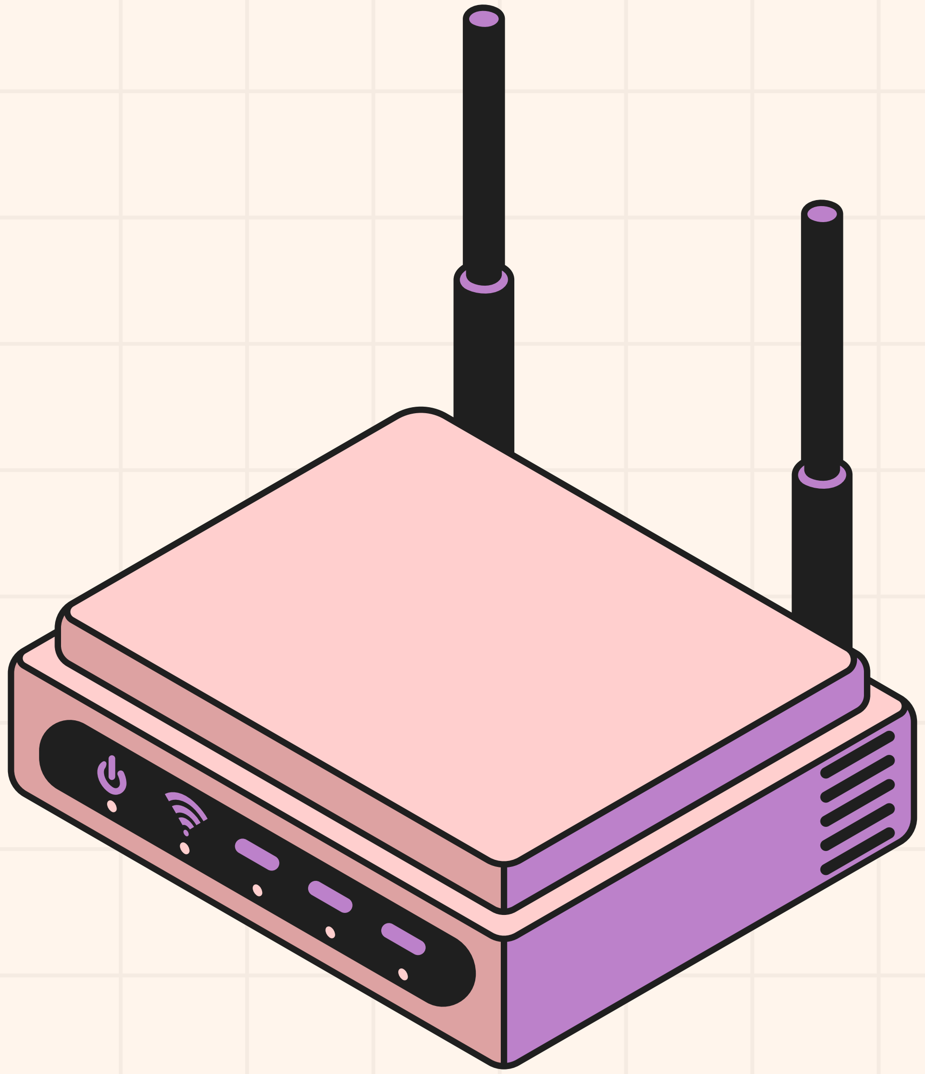
LAB TOPOLOGY

GOAL

Modeling of a duel-site network consisting of an HQ and a Branch. The setup includes WAN emulation, end-user LANs, and a dedicated management segment.

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



LAB TOPOLOGY

Management IP Addresses

Management access was established using the following IPs:

- HQ GUI: 172.16.1.10:8443
- Branch GUI: 172.16.1.11:8443
- Local PC: 172.16.1.1 (VMnet1)

HQ Site

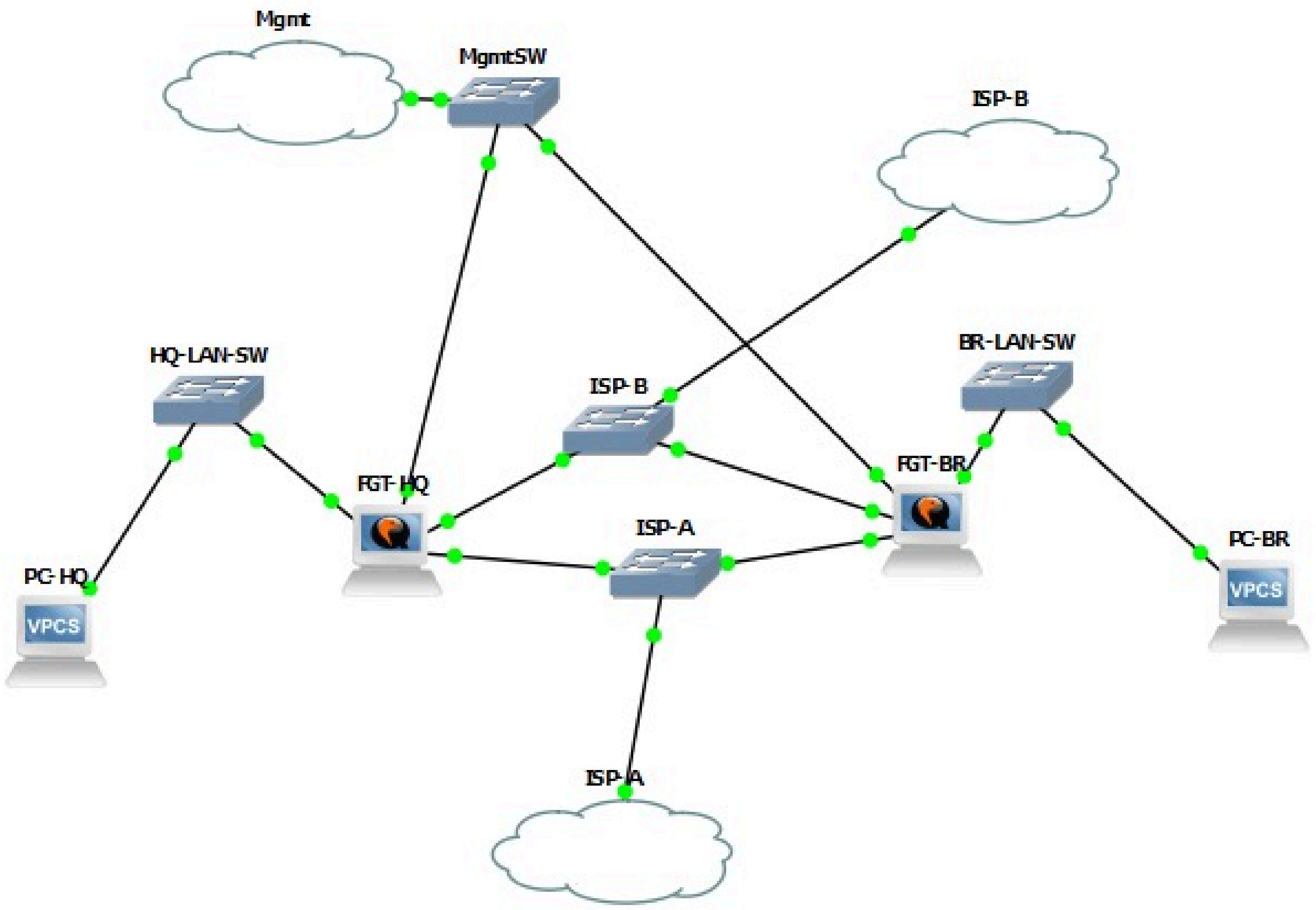
- FGT-HQ (Firewall of HQ)
- HQ-LAN-SW(HQ SWITCH)
- PC-HQ(TESTING CONDUCTIVITY)

Branch Site

- FGT-BR(Firewall of branches)
- BR-LAN-SW(BR SWITCH)
- PC-BR(TESTING CONDUCTIVITY)

Wan Simulation

- ISP A and ISP B providing duel wan path



WHAT WE SUCCESSFULLY BUILT

1.LAN Configuration

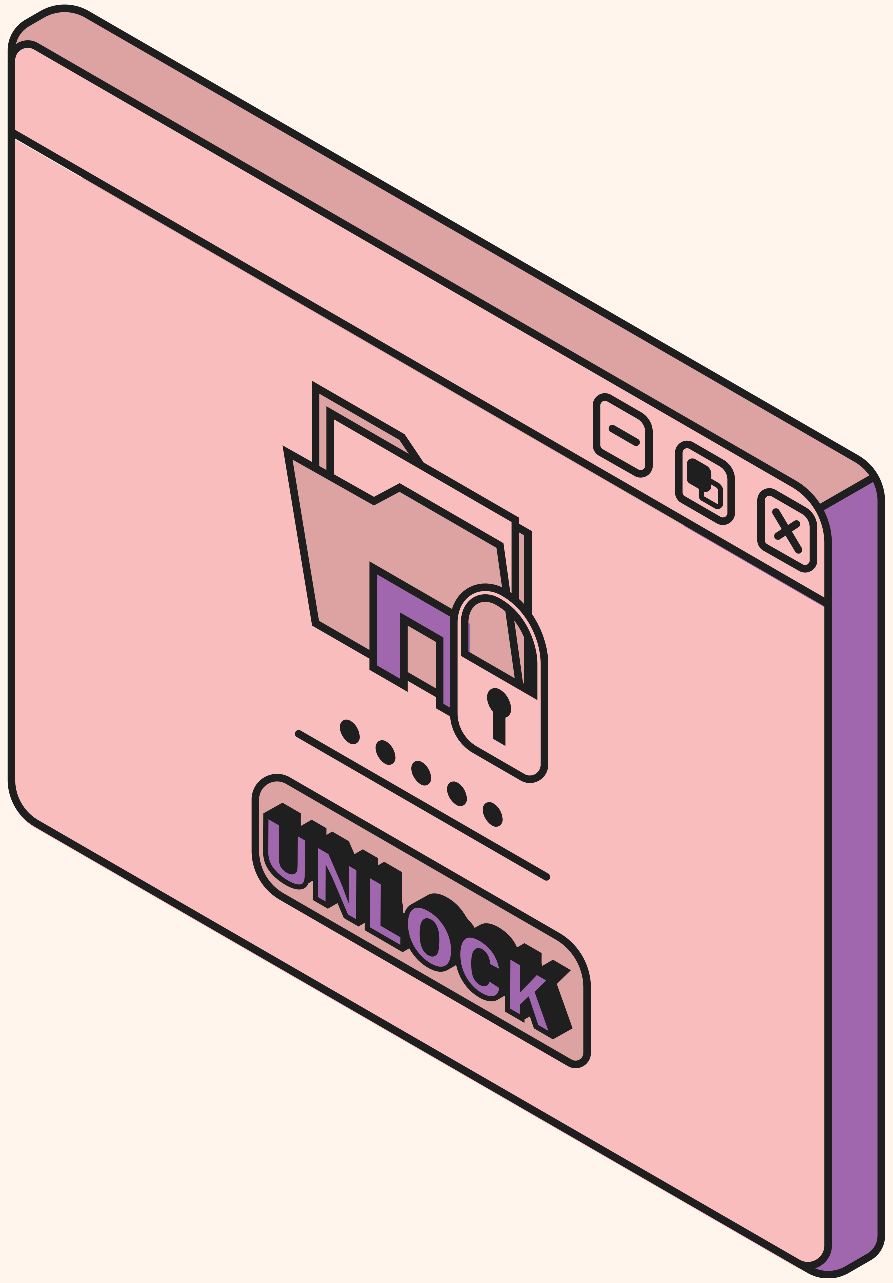
- HQ LAN: 10.0.1.0/24
- Branch LAN: 10.0.2.0/24
- PCs assigned:
    - HQ PC: 10.0.1.10 / gateway 10.0.1.1
    - Branch PC: 10.0.2.10 / gateway 10.0.2.1

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.



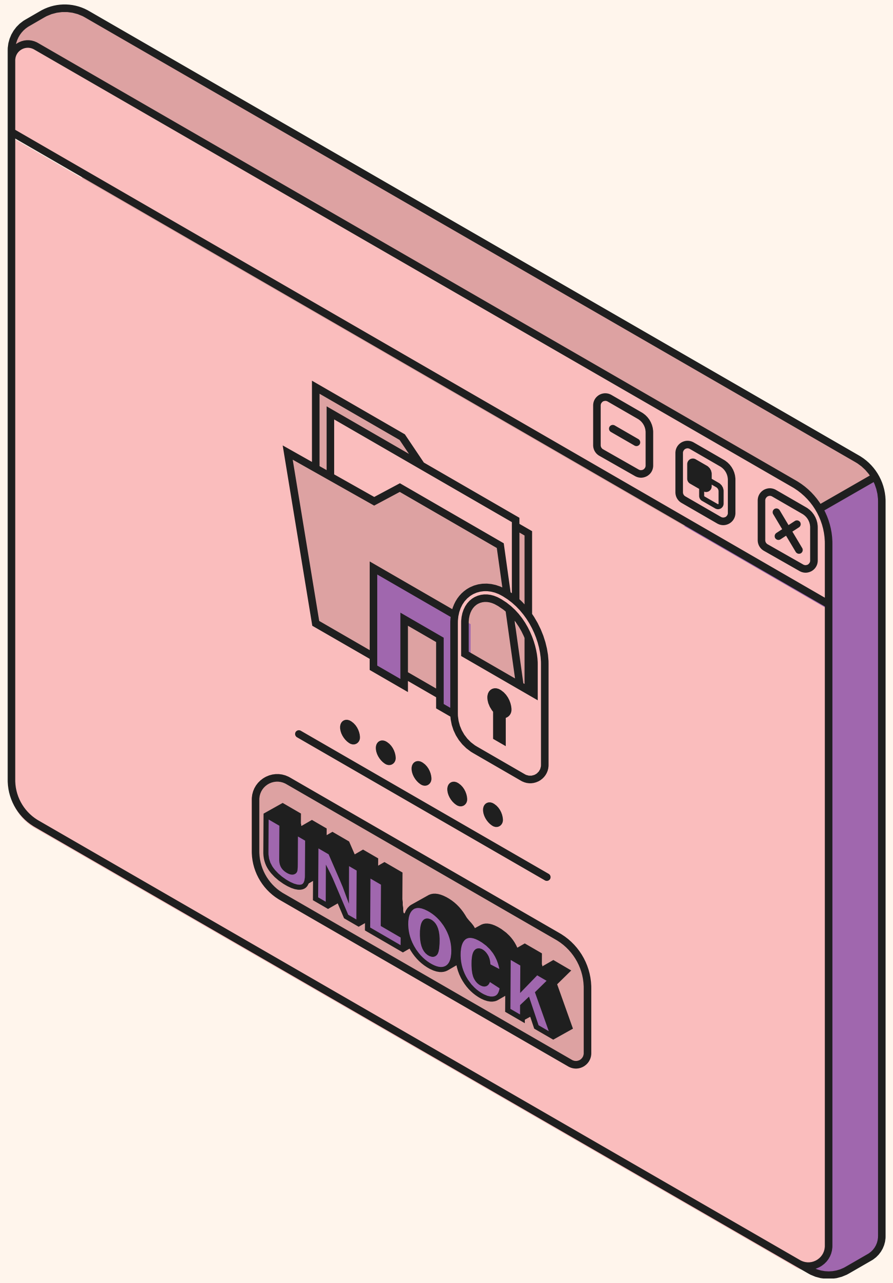
WHAT WE SUCCESSFULLY BUILT

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.

WHAT WE COULD NOT COMPLETE

(because of FortiGate VM image limitations)

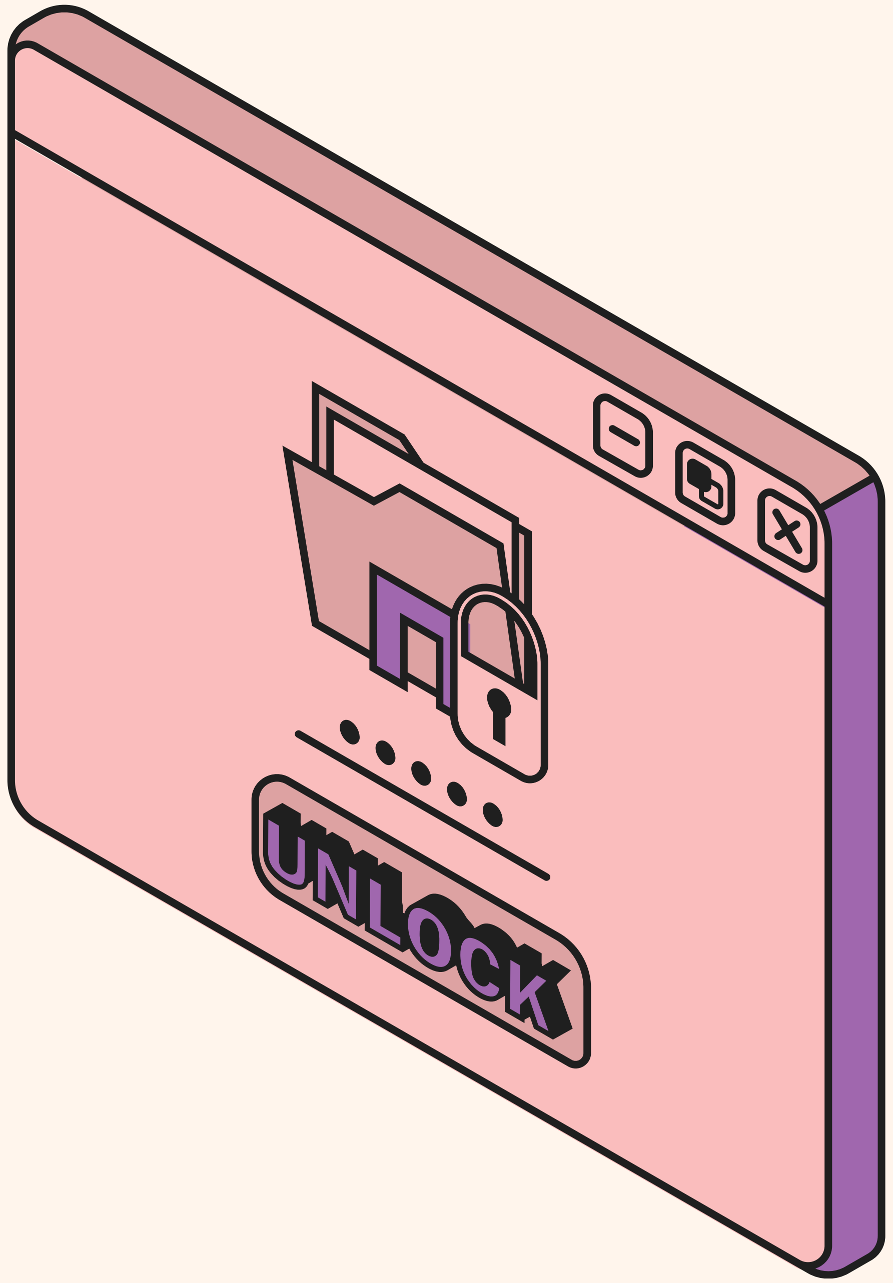
3. Full Cryptography (AES)

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

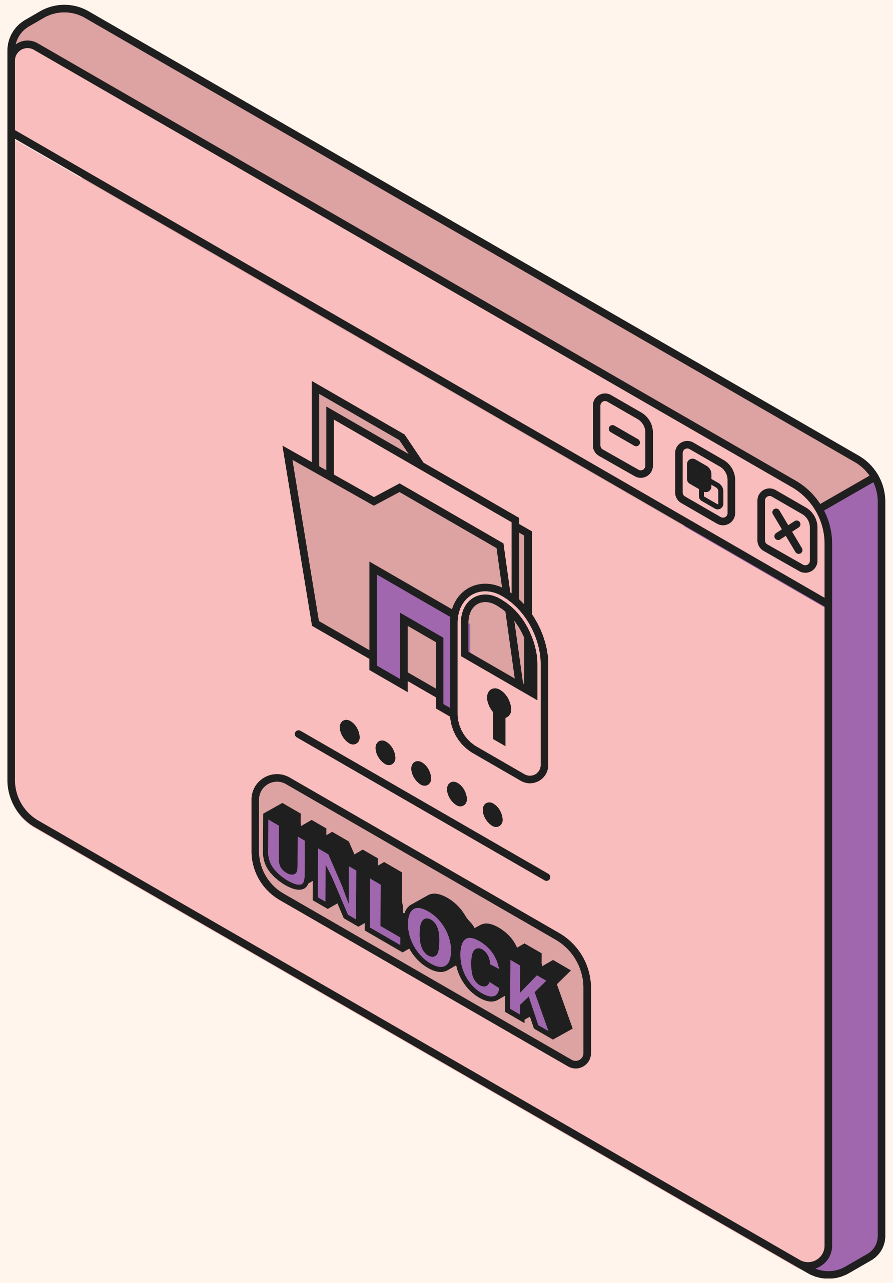
The FortiGate qcow2 image used in the lab was a demo/minimal KVM build, which lacked several essential FortiOS modules.

Limitations of the demo image:

- SD-WAN engine not included
- SSL-VPN services disabled
- Limited cryptography (no AES)
- Missing advanced CLI/diagnostic tools
- Required background listener processes unavailable
- Not an officially licensed FortiGate VM

Solution:

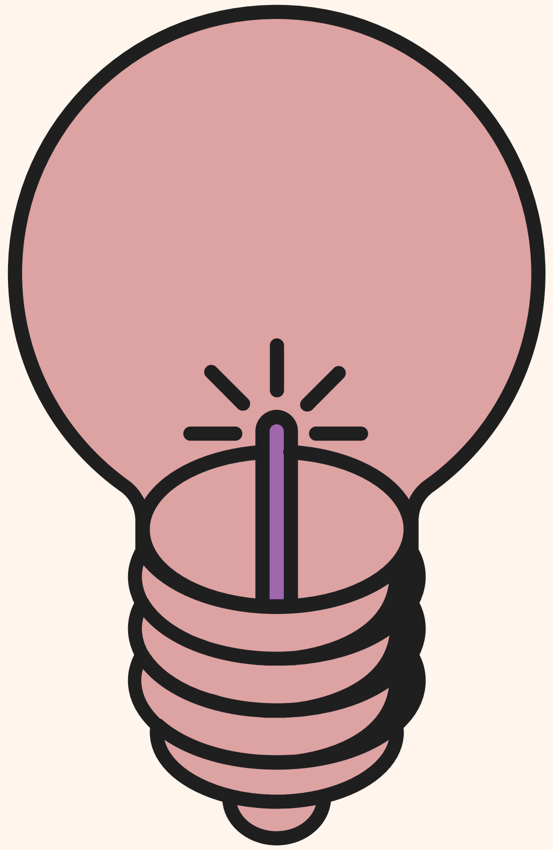
Use the full-featured, licensed Fortinet VM image:
FGT_VM64_KVM-v7.x.x-FORTINET.out.kvm.zip



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

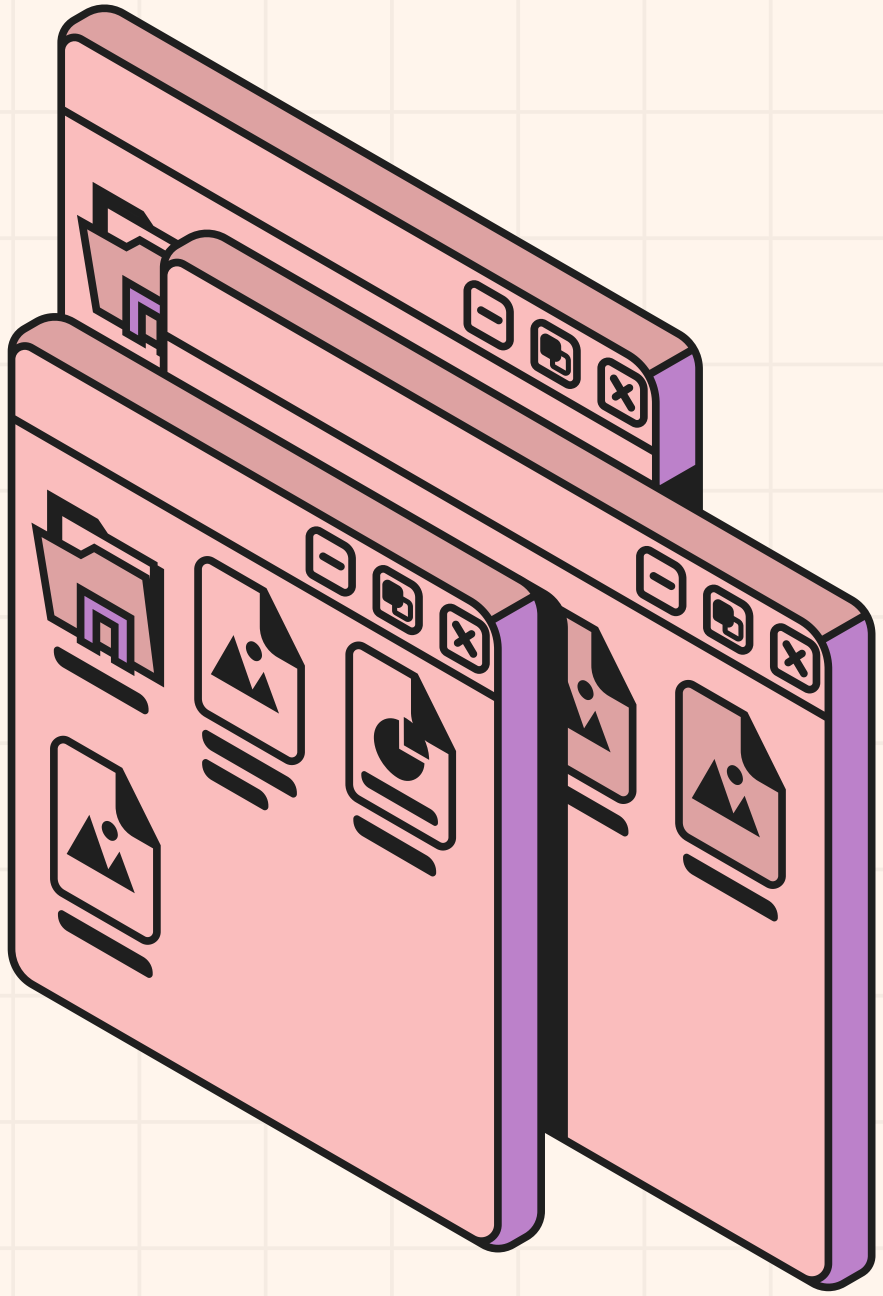


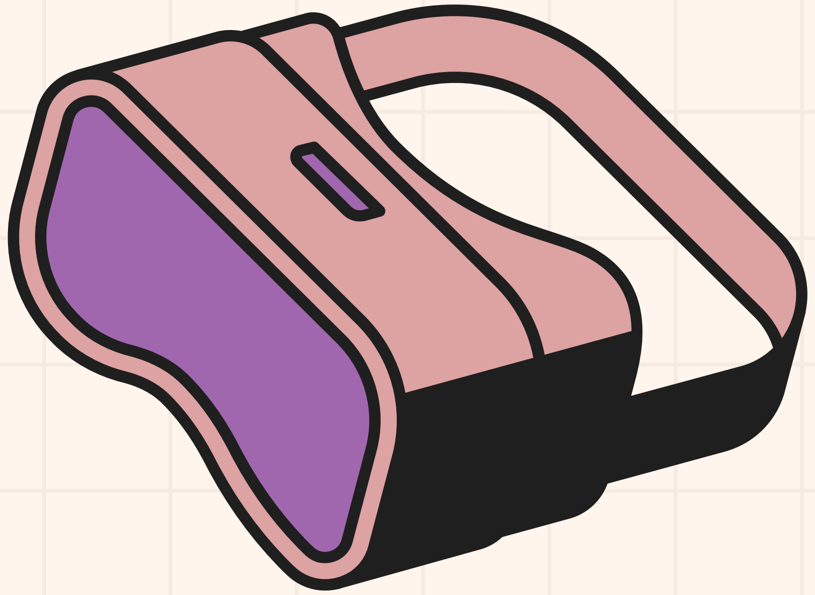
CONCLUSION

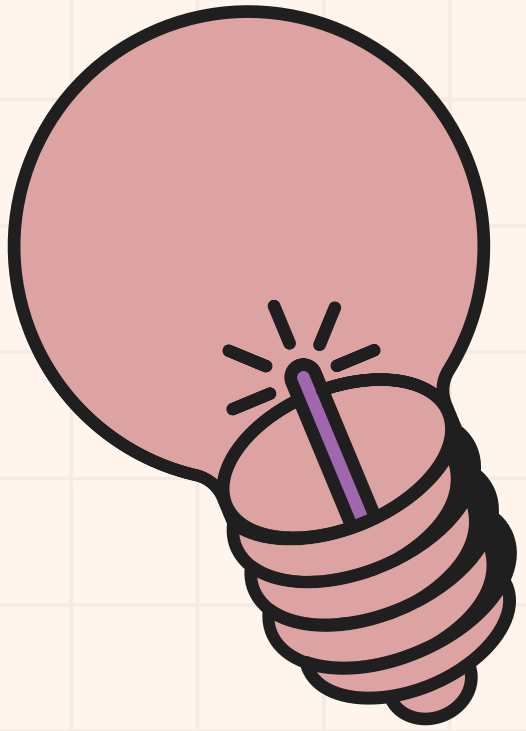
We successfully built the core VPN topology using GNS3 and FortiGate:
LAN environment
WAN simulation
Full IPsec tunnel HQ ↔ Branch
Management access & GUI functionality
But due to FortiGate VM license restrictions:

- SSL-VPN
- SD-WAN
- Advanced crypto

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







THANK YOU