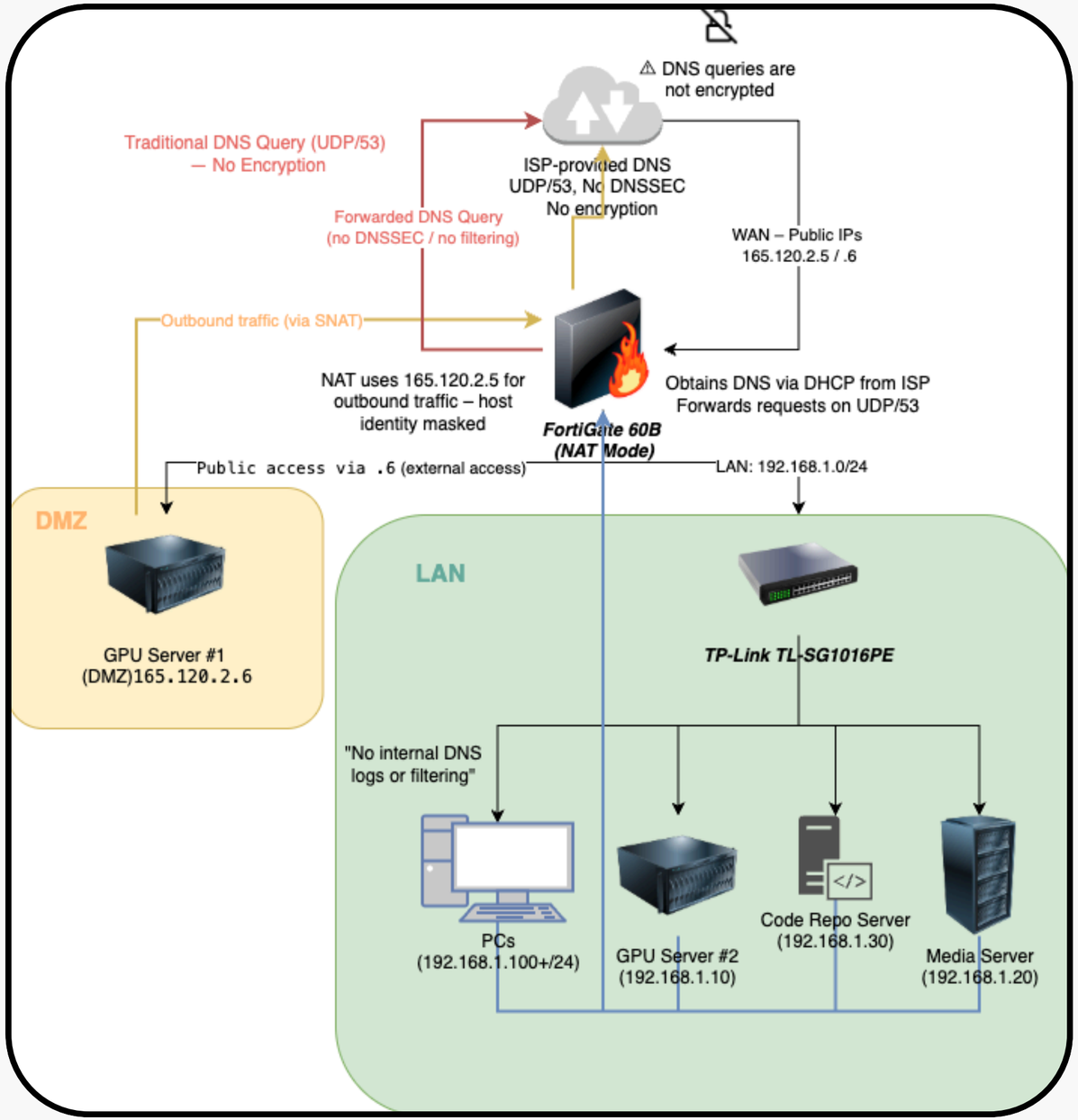
Dominicus Adjie Wicaksono - 40352799

Task 1

Discuss and compare how different DNS arrangements can be applied to the network

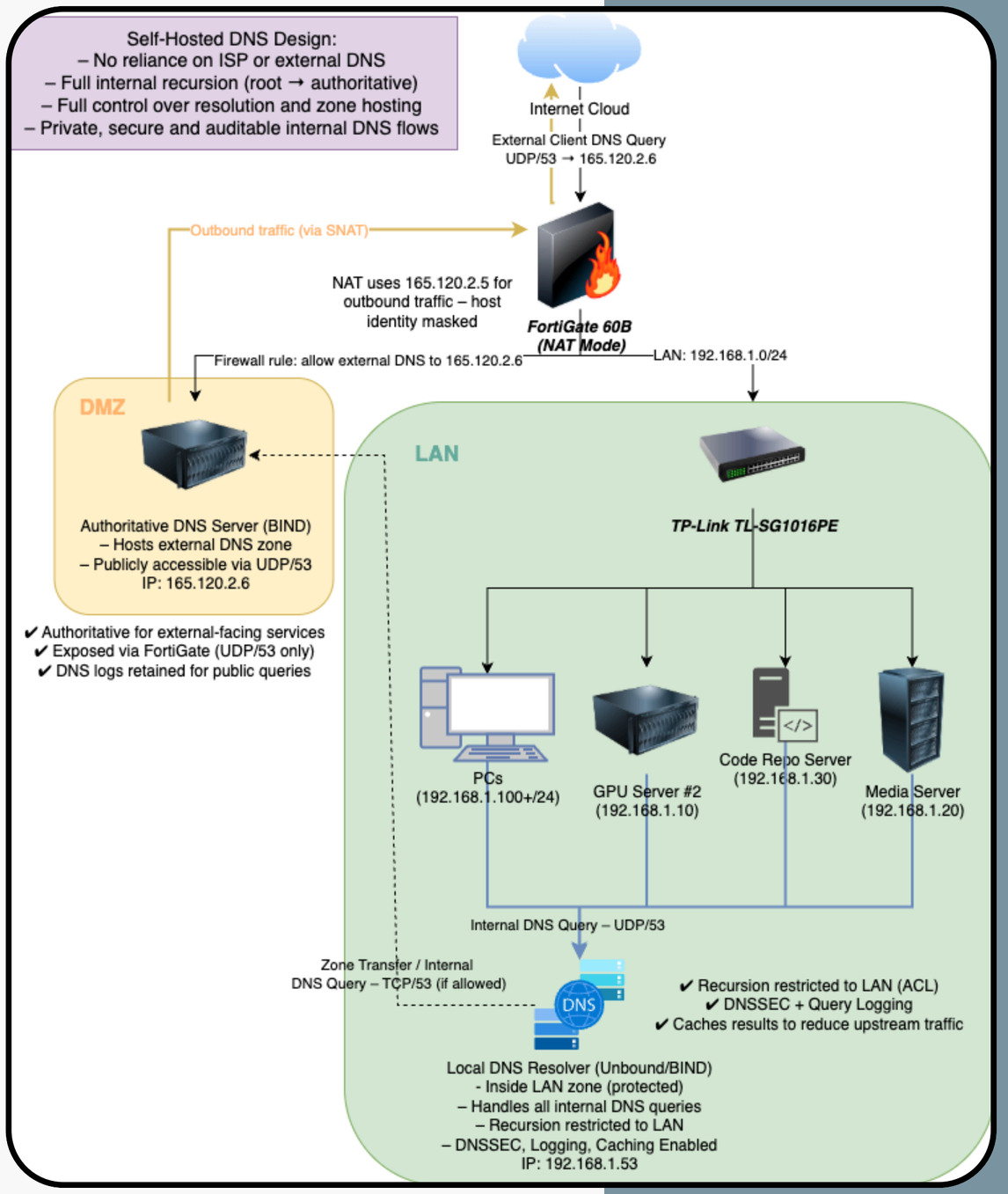
ISP DNS Resolution (Simple Forwarding via FortiGate)

- All internal hosts use DHCP from FortiGate 60B (192.168.1.0/24).
- FortiGate obtains DNS settings automatically from the ISP.
- DNS requests from the LAN are forwarded on UDP port 53.
- FortiGate performs Source NAT using 165.120.2.5.
- No internal DNS server — no caching, filtering, or logging.
- ISP DNS does not support DNSSEC or encryption (queries sent in cleartext).
- DNS traffic leaves the LAN and passes through the NAT firewall to the ISP's DNS server.



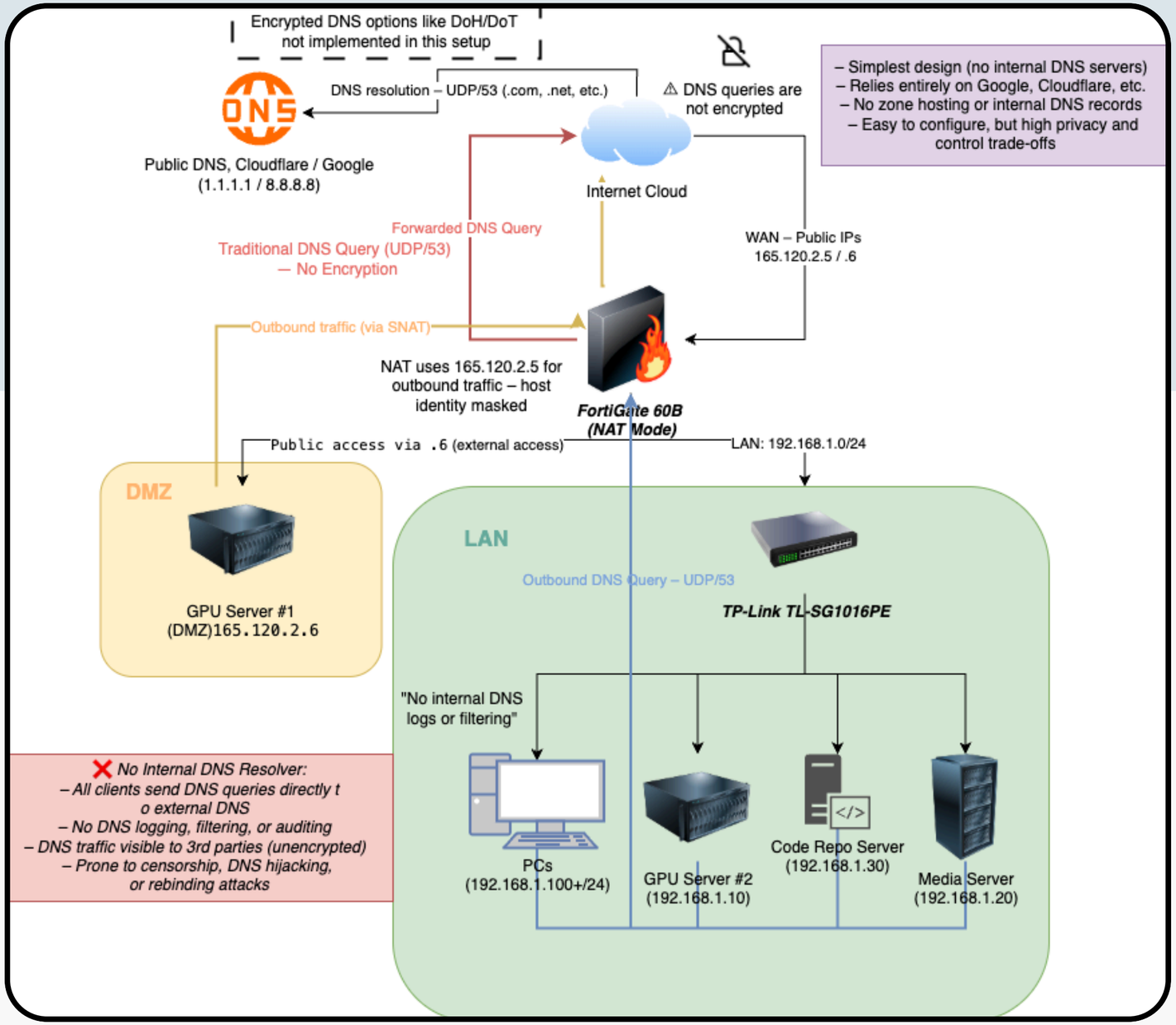
Self-Hosted DNS (Internal + Authoritative)

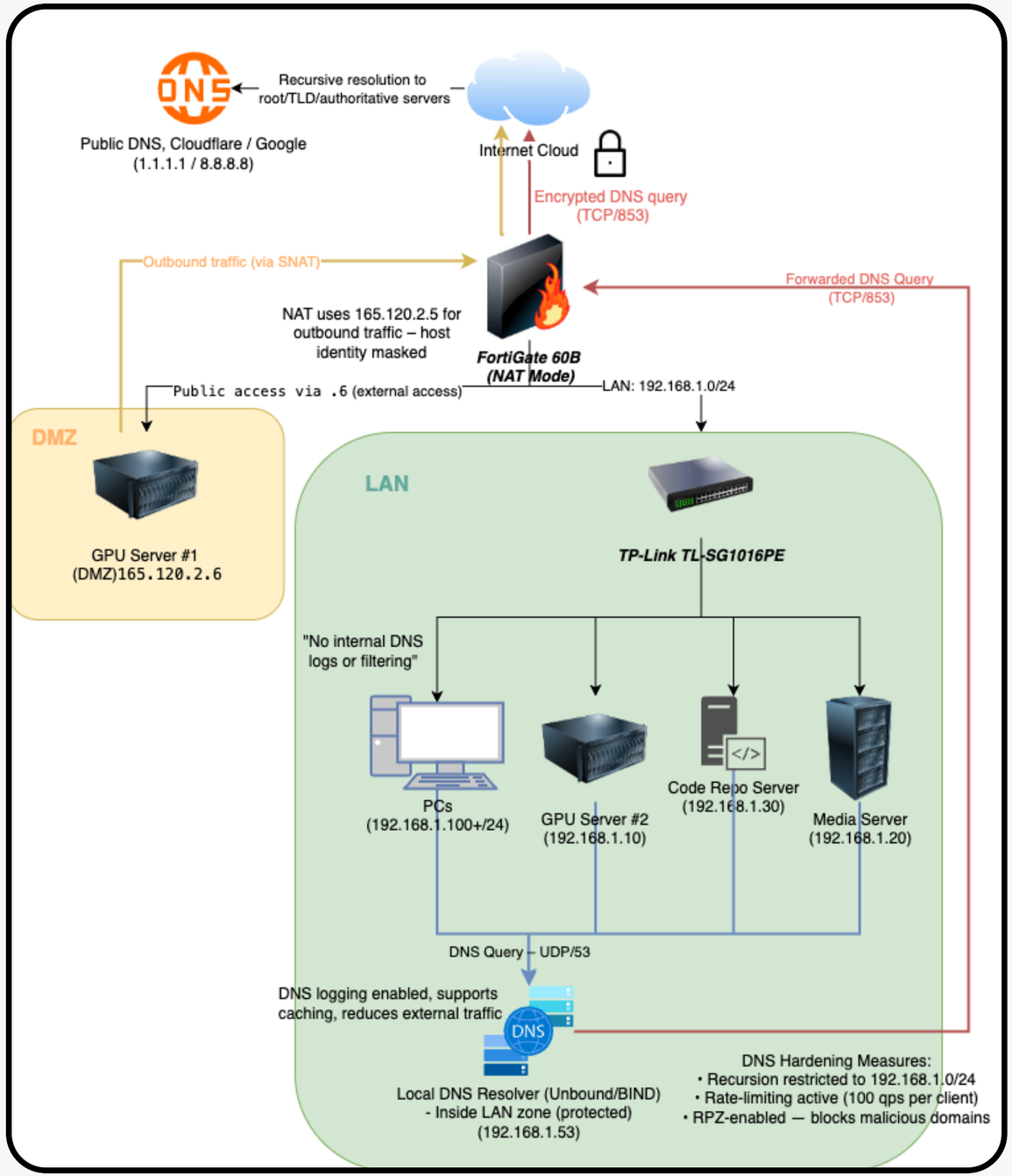
- Internal DNS resolver (192.168.1.53) handles all LAN queries
- Full recursion enabled with DNSSEC, caching, and query logging
- Authoritative DNS server exposed to Internet (UDP/53 → 165.120.2.6)
- Firewall permits inbound DNS only to DMZ server
- No reliance on ISP DNS – improved privacy and control
- NAT via FortiGate masks internal host identities



Public DNS – No Internal Resolver

- No internal DNS server
- Direct DNS queries to public resolvers
- No logging or filtering
- Unencrypted (UDP/53)
- Privacy, security, and control issues



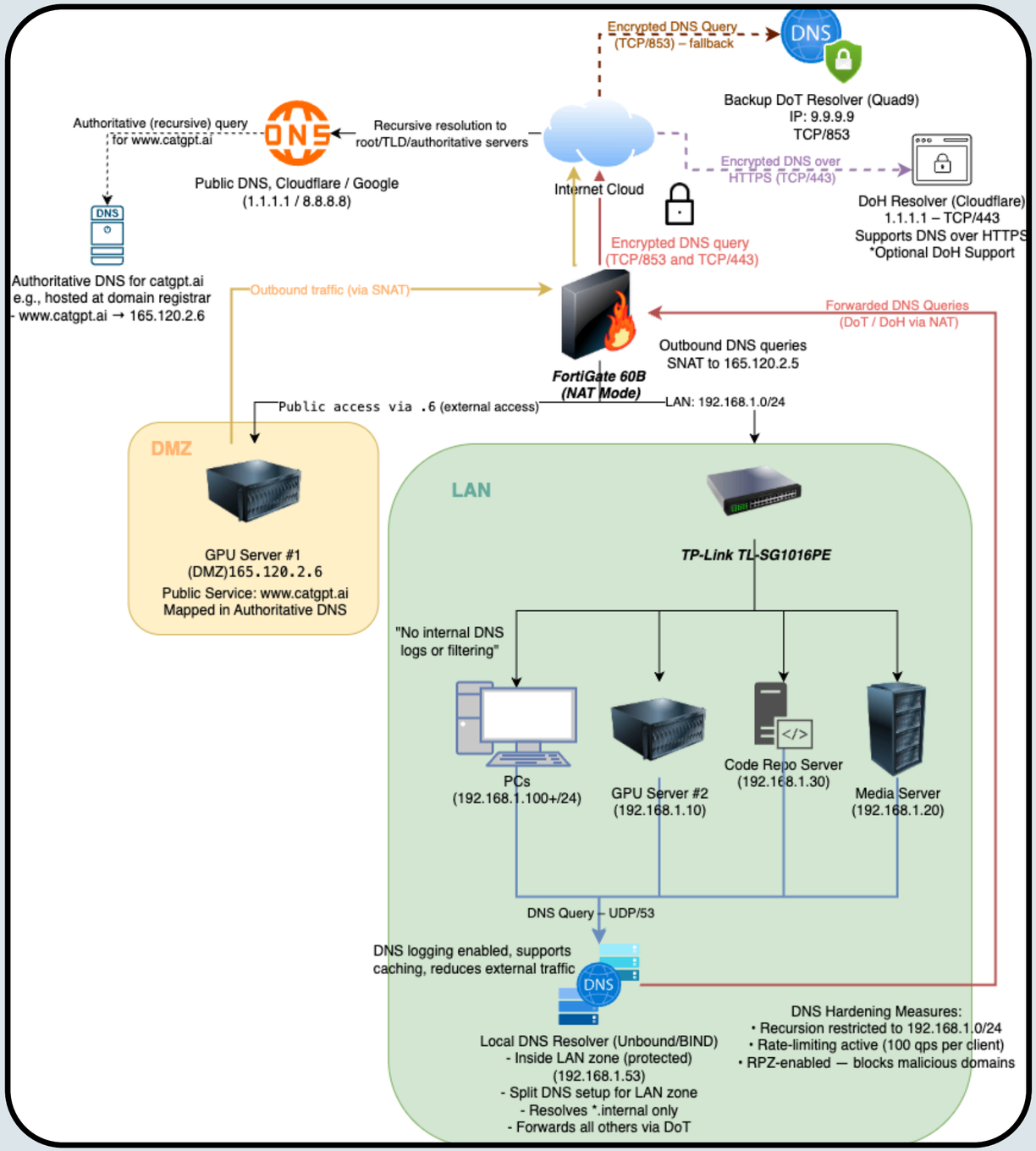


Hybrid DNS

- Plaintext DNS vulnerable to spoofing, hijacking, and MITM
- No source validation or integrity checking
- No internal DNS means no domain filtering or response policy
- DNS logs absent – attacker queries go unnoticed
- Ideal target for C2 traffic, DNS tunneling or phishing

Split DNS - Recommendation

- Purpose: Separate internal and external DNS resolution
- Internal DNS Resolver:
- Handles internal domains (e.g., *.internal)
- Forwards public domains securely (DoT/DoH)
- External DNS:
- Public records (e.g., www.catgpt.ai) resolved via authoritative DNS
- Security Gains:
- Internal visibility, logging, and control
- External exposure is minimized and encrypted



Dominicus Adjie Wicaksono - 40352799

Task 2

Analyse and compare the security implications of using different DNS arrangements

Subtask 1: Firewall Policy Table

DNS Setup	Required FortiGate Policies
1. ISP-Forwarded DNS	Allow outbound UDP/53 from LAN to ISP DNS; minimal filtering; no internal DNS rules needed.
2. Internal DNS + DMZ Authoritative	Allow UDP/53 from LAN to 192.168.1.53; Allow TCP/853 outbound to public resolvers; Allow inbound UDP/53 to DMZ DNS at 165.120.2.6; Deny all DNS to/from unauthorised destinations.
3. Public DNS Direct	Allow outbound UDP/53 from LAN to any; block DNS from DMZ; risks uncontrolled destinations.
4. Split DNS (Hybrid, Diagram 2)	Allow UDP/53 to 192.168.1.53; Allow TCP/853 to public resolvers; Inbound UDP/53 to DMZ 165.120.2.6; Deny DNS from DMZ and block outbound DNS to untrusted IPs.
5. Split DNS (Flow-level, Diagram 5)	As above, but explicitly add rate-limiting, DoT/DoH filtering, and restrict fallback resolvers.

Subtask 2: CIA Risk Comparison Table

DNS Setup	Confidentiality	Integrity	Availability
ISP-Forwarded	❌ No encryption; ISP can monitor traffic	❌ Susceptible to spoofing (no DNSSEC)	✅ High, but with poor control
Internal + DMZ	✅ Internal queries hidden	✅ DNSSEC + ACLs available	✅ Caching + fallback resolvers
Public Direct	❌ Exposes client IPs; no control	❌ Easily spoofed	✅ But lacks filtering or DoS protection
Split DNS (Hybrid)	✅ Internal/private separation	✅ DNSSEC + RPZ filtering	✅ Resilient + secure resolution paths
Split DNS (Flow-level)	✅ Strongest (DoT/DoH, ACLs, RPZ, logs)	✅ Full validation and blocklists	✅ Rate limiting + fallback support

Subtask 3: DNS-Based C&C Implications Table

DNS Setup	Detection and Prevention of DNS C&C
ISP-Forwarded	❌ No visibility; hard to log/analyse
Internal + DMZ	✅ Internal resolver can log & detect anomalies
Public Direct	❌ Zero logging/control; DNS tunneling undetectable
Split DNS (Hybrid)	✅ Internal logging + RPZ can catch known bad domains
Split DNS (Flow-level)	✅ Best setup: logs + rate-limiting + RPZ + anomaly detection + encrypted outbound

Subtask 4: Final Recommendation

Recommend Split DNS (Diagram 5) as most suitable for CatGPT, justified by:

- Internal visibility (local resolver logs)
- Encrypted outbound DNS (DoT / DoH)
- External DNS control (authoritative server in DMZ)
- RPZ filtering, rate limiting, and recursion restriction
- Mitigates C&C risks and preserves C-I-A principles