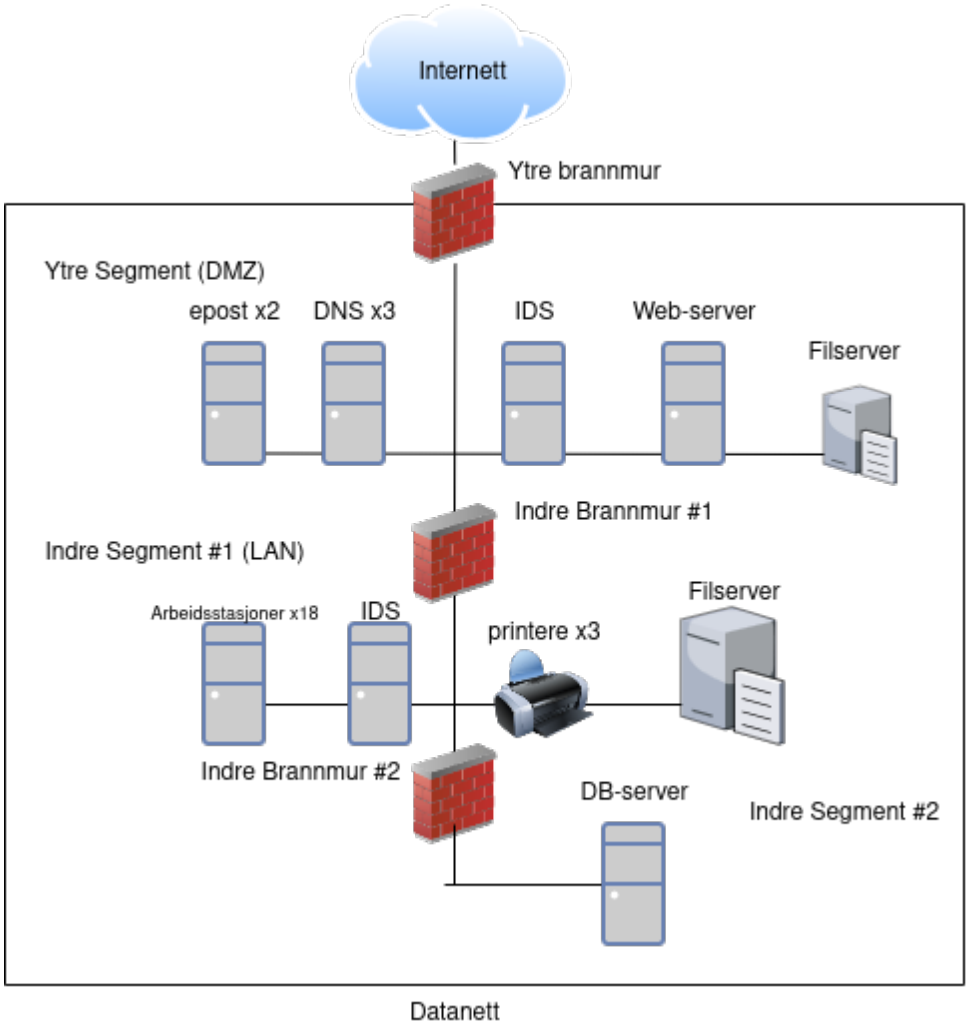
# Oblig 3 Mats Andersen (matande)

**1)** iptables -A FORWARD -p tcp  -d 192.168.56.23  --dport 21 -j ACCEPT
iptables -A FORWARD -p tcp  -s 192.168.56.23  --sport 21 -j ACCEPT

**2)** xY688ASSu27 er passordet.

**3)** TLS 1.3 stoetter fremoverhemmelighold, fordi den baserer seg paa en kryptoprotokoll som etablerer og utveksler hemmelige, symmetrisk krypterte (DH) oektnoekler, hvis autentisitet er basert paa tjeners private noekkel.

**4)**



Her foelger en kort forklaring: Kun det ytre segmentet (DMZ-sonen), bak den ytre brannmuren, er tilgjengelig fra internett. Derfor har vi her DNS-serverne, epost-serverne og web-serveren. Jeg har ogsaa valgt aa plassere filserveren her, dersom det er noen filer som maa vaere tilgjengelig fra eksterne enheter. Denne krever, selvfoelgelig, eksepsjonelt streng tilgangskontroll. Jeg har ogsaa valgt aa plassere en IDS her, som er en tjener (HIDS); det er en honningkrukke.

Bak den foerste indre brannmuren har vi LAN-nettverket hvor arbeidsstasjonene staar. Disse har tilgang til printerne og en intern filserver, for sikker deling av informasjon lokalt paa nettet. Her er det ogsaa en IDS, som er en tjener (HIDS); det er en honningkrukke.

Bak den andre indre brannmuren staar database-serveren. Denne inneholder sensitiv informasjon.

**5)** Anomalibasert IDS, til forskjell for signaturbasert IDS, baseres (trenes) paa normal atferd. Vha. intelligent maskinlaering kan denne detektere unormale atferdsmoenstre i nettverket, og rapportere om dette. Problemet er at dette kan gi falske positive, og at det krever tungt utstyr.

**6)** En honeypot er en slags “felle” i systemet som ser ut som noe interessant, men hvis formaal egentlig kun er aa varsle om og laere fra inntrenginger. Dvs. at den vanligvis ikke brukes internt i systemet.

**7)** IDS paa utsiden: Mye stoey og krever derfor stor prosesseringskraft, men mulig aa detektere inntrenginger og forstyrrelser tidlig. IDS paa innsiden: Dersom alarmen gaar, saa er paa en maate allerede “for sent”, i den forstand inntrengeren allerede er inne. Fordelen er at man kan studere inntrengers atferd og teknikker mer noeye, og varsle de indre segmentene.

**8)** Moerke IP-adresser er aldri i bruk; ingen skal ved noen anledning koble seg paa disse. Dersom noen gjoer det, er det et sikkert tegn paa mistenksom aktivitet. Dessuten reduserer disse antall mulige IP-adresser, saa angrepsflaten blir dermed mindre.

**9)** VPN-er gjoer det mulig for ansatte aa opprette en sikker, skjult og kryptert “tunnel” til det interne nettverket. Logisk sett er det som om den ansatte er paa kontoret sitt.