Universitetet i Sørøst-Norge
Institutt for realfag og industrisystemer

Fakultet for Teknologi, Naturvitenskap og Maritime fag

Innleveringsoppgave

Nettverk og sikkrerhet/TSD2090K-1 25V

23.03.2025

[Salim Zakaria Ahmed/241775]

Nettverksdesign Oppgave

Innholdsfortegnelse

Om bruk av KI-verktøy

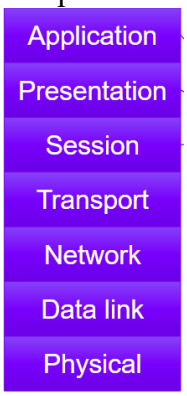
I denne oppgaven er det eneste KI-verktøyet som er brukt ChatGPT. Dette var så stor og fri oppgave som trengte en grundig gjennomgang og begrunnelse for hver komponent. Derfor brukte jeg ikke KI direkte til oppgaven. Man må være veldig obs på det. Jeg brukte KI for oppsett av teksten min. jeg brukte den for å få en liste av relevante begreper. Jeg fikk brukt disse begrepene til praksis som fikk meg til å forstå mer enn det KI hadde lært meg. Jeg brukte den også på definisjonene, noe som er vist og underbygd i rapporten.

Innledning

I denne oppgaven er jeg gitt oppgaven til å designe et nettverk til en bedrift for 4 kontorer spredt rundt til 4 kontorer. Jeg har tatt for meg en bank. Derfor må nettverket være sikkert. 3 av kontorene skal kobles sammen via internett, mens den siste skal kobles med egne leide linjer. 2 av kontorene skal ha 50 ansatte, mens de 2 andre skal ha 10 ansatte. Man må selv gjøre en avgjørelse på hvor mange ansatte som er koblet til per switch. Serverparken skal være plassert i ett sted, men alle må kunne jobbe seg mot den. Siden dette er en bank må serverparken være plassert på et sikkert sted.

Denne banken skal håndtere alle oppgavene til en bank. Inneholde data for kunders informasjon og transaksjoner. Man må også ha i en backupserver i tilfelle serveren ryker. Også en webserver som kundene kan bruke for å logge seg på nett siden. Som sagt må den utestenge hackere og lekaskje av sensitiv informasjon. Kommunikasjonen mellom bedriftene må være kostnadseffektiv.. Jeg skal også gjøre meg noen tanker rundt sikkerhetsrisikoen.

Jeg har tatt i bruk ulike nettverks komponenter som brannmur, switch, router, VPN og servere. VPN er en «tunnel», [1] *LAN++.pptx*. VPN er en kryptrerer datapakkene i trafikken som gjør kommunikasjonen mer sikker mellom 2 nettverk. Brannmur er en sikkerhetsenhet som passer på at data pakkene går der de skal uten at noe eksternt kommer i veien. En server tar vare på kritiske data. «kraftig datamaskin som gir brukeren tjeneste», [3] *chatGPT,10.03.2025*. En router er den som sender datapakkene i riktig sted, det er det som sammen handler alle nettverkene. En sub switch er der alle enhetene er koblet til. Hovedswitch er en samling av alle sub switchene og sender datapakken til router. Nettverket skal følge OSI-modellen.



OSI-modellen

[5]Intro.pptx, Olaf presentasjon (20.02.25)

Hovedkapitlene

Valg av Kostnad og sikkerhet

Jeg har tatt bevisste valg i forhold til dette nettverkdesignet. Jeg har valgt å ha 50 ansatte på kontor

1 og 3, mens kontor 2 og 4 har 10. Kontor 4 har er koblet med leide linjer. Det er 5 enheter per sub Switch. Kontor 4 har 10. Som sagt skal den være veldig sikker, samt kostnadseffektiv. Som man ser i vedlegget har jeg valgt å ha 5 enheter per switch. Dette vil koste mer. Det vil bli flere enheter å ta styr om. Men jeg valgte 5 per switch siden, dersom en sub switch ryker så blir konsekvensen mindre på kontoret. På kontor 4 tok jeg 10 siden det er et lite kontor. Siden bank er alltid oppdatert sanntid, må den alltid kjøre. Derfor kan jeg også velge og prioriterte hvilken sub switch som er viktigere enn andre. Et annet valg som er bevisst tatt er valget av en VPN kobling gjennom alle. Man kunne hatt egne leide linjer som er koblet fysisk, men kontorene er rundt i landet og dette er mye dyrere. Dette blir bruk i flyplasser og internasjonale banker, siden dette er kritisk. Sistnevnte begynner å bevege seg mot VPN som gir ganske sikker informasjon. Jeg har valgt VPN gjennom alle fordi banken er i Norge, og ikke så stor bedrift. Som man ser i vedlegget har ikke jeg laget alle sub switchene for kontor 2 og skrevet kun hovedswitch. Dette er på grunn av å vise forskjeller mellom kontor med 50 ansatte og 10 ansatte.

Jeg subnetter nettverket. Det er hvordan jeg deler opp nettverket mitt i mindre deler for sikkerhet. Subnetting isolerer kontorene i nettverket ved å «gruppere» nettverket med IP-adresser. Det gjør nettverket mer sikkert. Dersom serveren svikter er det viktig med en rask backup server, som bør være lett tilgjengelig for kontor 1. Alle kontorene har tilgang gjennom VPN i hver router. Denne beskyttelsen fra kontor 1, med så mange ansatte sparer derfor penger.

Hovedkomponentene

Switch

De ulike enhetene som er brukt er laptop, printer og stasjonær pc, siden dette er en bank. Disse går opp til en switch og distribuerer riktig pakker i nettverket. Jeg har brukt sub switcher, som er flere switch som er koblet til hoved switch. hoved switch tar imot alt og sender dataen videre i trafikken. Dette ser man i kontor 1 og 3 i vedlegget. Videre går pakkene da til en router. Som sagt har kontor 2 det også, men for å vise forskjell på ansatte så satte jeg ikke enheten der men kun skrev det. Serverparken har en egen switch som sørger for at kommunikasjonen er effektiv mellom server og kontor. Siden dette er en bank så er hovedfokuset sikkerhet. Kun autoriserte medlemmer skal kunne ha tilgang til de ulike serverne. For å forbedre nettverkskommunikasjonen bør man dele nettverket opp. Det kan gjøre med subnetting. Det gjør det mer strukturert. Hvert kontor kan ha sin egen subnett. En bank trenger subnett siden belastinger går raskere og en bank håndterer sanntidsdata.

IP-adresser

Nettverket mitt viser hvordan IP-adressene er delt i nettverket. For å forbedre nettverkskommunikasjonen bør man dele nettverket opp. Det kan gjøre med subnetting. Det gjør det mer strukturert. Hvert kontor har sin egen IP-adresse. En bank trenger subnett siden belastinger går raskere og en bank håndterer sanntidsdata. I mitt diagram er kontor 1 koblet til Serverpark så det er samme adresse mellom dem. Det er 192.168.1.0/24 som forteller oss at det er 253 adresser tilgjenlig i kontor 1 og serverpark. Subnettmask forteller oss om hvilken del som er hostadresse og nettverksadresse (der 255.255.255.0, de 3 første bitsene er nettverk og siste er enhet). 192.168.1.0 ikke er mulig, 192.168.1.255 er broadcast og en routeren har en IP-adresse som eks. 192.168.1.22. En PC for eksempel på kontor 1 kan ha IP-adresse 192.168.1.13 for eksempel. Dette gjelder også kontor 2,3 og 4. Der deres subnett er 192.168.2.0/24(kontor 2), 192.168.3.0/24(kontor 3) og

192.168.4.0/24(kontor 4). Hver router for sin egen IP innenfor subnettet. Det er gateway, som er inngangen til en annet nettverk som kontor 2(192.168.2.1), som skjer gjennom routeren. Dersom måldestinasjonen til en kontoret er et eksternt nettverk blir datapakker sent gjennom et eksternt nettverk. Motsatt er da Interface utgangen fra ruteren. Ruter kan ha mange Interface for å koble til flere nettverk, som kan være virtuelt eller fysisk.

Router

Datapakkene blir sent til router. Dette er her trafikken mellom datapakkene blir sent mellom kontorene og nettverkene kobler seg sammen. Som man ser i designet mitt har jeg koblet dem sammen med en VPN. Der alle kontorer og serverpark kan kommunisere sammen uavhengig hvor i ladet de befinner seg. Routeren sørger ikke kun for traffikken mellom nettverkene, men også internett. Der det er en brannmur imellom for sikkerhet. Som man også ser i oppsettet mitt har hver kontor en router. Serverpark er koblet til router 1 fra kontor 1. Trafikken går gjennom denne «tunnelen» som krypterer filer og sørger for sikkerheten. Som sagt kan et nettverk som kontor 1 for eksempel kommunisere med internett.

Dersom måldestinasjonen var et eksternt nettverk ville datapakkene blitt sendt med WAN(Wide Area Network) med en IP-adresse. I designet mitt er trafikken mellom kontorene og internett brukt med VPN interface. Som man kan se blir Interfacen fra kontor 1 VPN3214. Routeren sørger ikke kun for traffikken mellom nettverkene, men også internett. Der det er en brannmur plassert imellom for sikkerhet. Som man også ser i oppsettet mitt har en hver kontor en router. Serverpark er koblet til router 1 fra kontor 1. Routingtabell kan bli illustrert i en tabell som forteller trafikken til datapakkene gjennom en protocol. I min routing tabell(tabell 1) er det vist datapakker sendt fra kontor 1 til kontor 2. tabellen forteller oss at all trafikk fra kontor 1 går gjennom en vpn adresse til en gateway med adressen 192.168.2.1 i routeren i kontor 2.

Network destination	Netmask	Gateway	Interface (VPN)
192.168.2.0/24	255.255.255.0	192.168.2.1	VPN3214

Tabell 1, Routing tabell fra kontor 1 til kontor 2

Brannmur

Brannmur er rundt i designet som skal sikre angrep fra eksterne enheter. I kontor 1 og 3 har jeg brannmur mellom sub switch og hovedswitch for ekstra trygghet siden det er de 2 store kontorer. Kontor 4 har sin egen brannmur for interne sikkerhet, siden den kun er koblet med VPN. Som sagt kan kun autoriserte ha tilgang til serverparken, derfor er det en brannmur foran den.
Siden brannmuren er designet til å forhindre uønsket trafikk må den følge noen regler, for å holde kontroll og sikkerhet. Prossesene skjer i ip-adressene, proter og protokoller som opererer i OSI lag 3, 4 og 7. Brannmuren skiller trafikken med allow og deny. OSI lag 3 brukes når brannmuren filtrerer IP-adressene sin kommunikasjon. OSI lag 4 skiller mellom hvilken porter som er tilgjenlig. I OSI lag 7 så tar brannmurene en nærmere titt på innholdet av datapakker.
Siden det er en bank med en webserver for kunder så er det tillat HTTPS port 443 (TCP)for sikrere tilagang. enn port 80 HTTP. Eksempel er allow proto tcp from 192.168.2.0/24 to any port 443. Det tillater subnettet til å bruke sikrere nett.
VPN trafikken skal kunne gå gjennom brannmurene for kommunikasjon mellom dem. Tillat VPN trafikk på port 1194 for UDP.

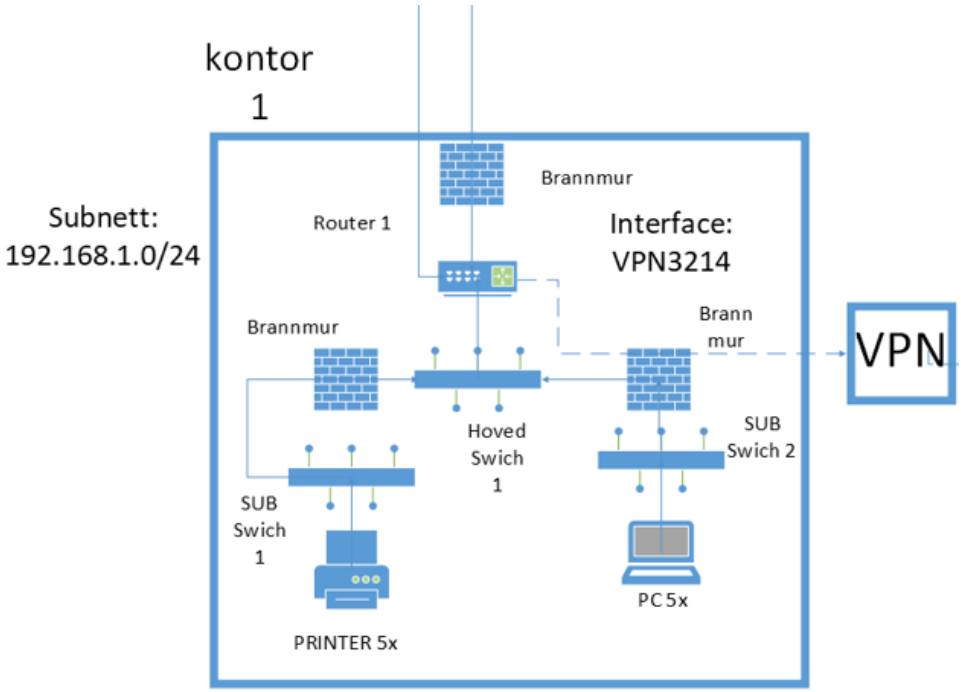
Blokker all uønsked trafikk og man kunne tatt fra spesifikke IP adresser som mistanke om svindel. Det hadde blitt deny from 202.3.224.7.

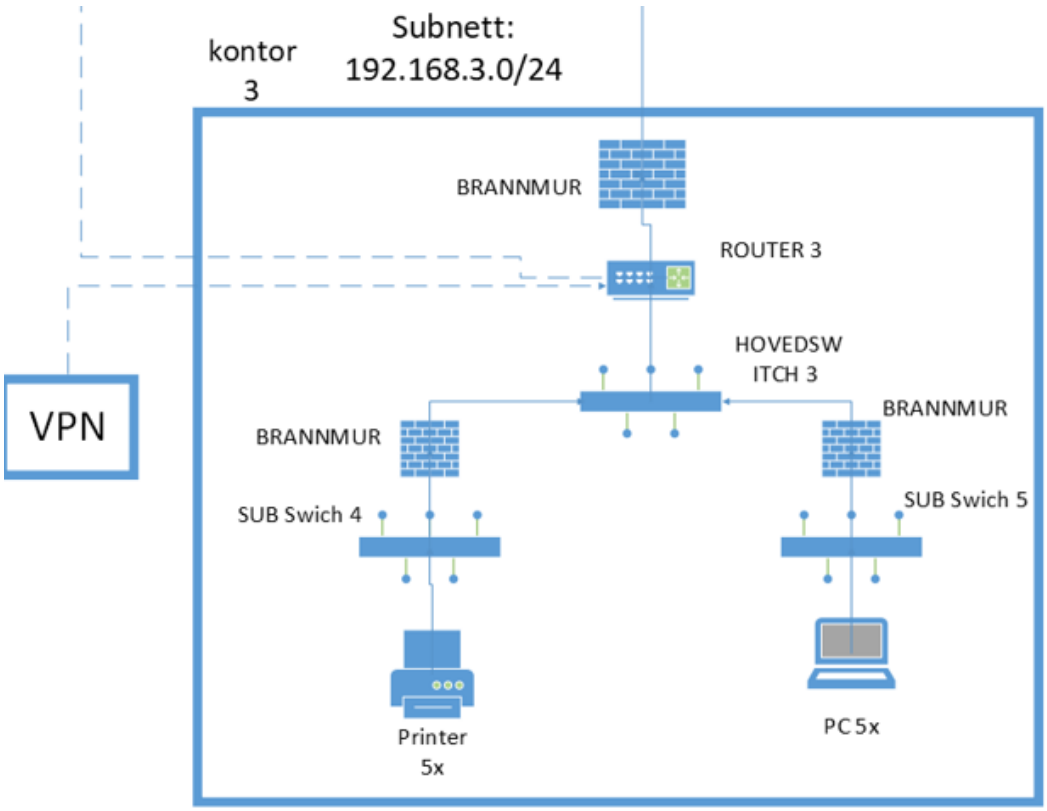
Server

Serverparken har 4 servere i modellen min. Databaseserver, webserver, transaksjonsserver og backupserver. Databasen har data om all kundeinformasjon og transaksjons historikken. Transaksjonsserver er der sanntids transaksjoner skjer, som tatt ut penger. Backupserver kjører dersom noe går galt, og tar alltid vare på kritiske og sensetiv data. Flere bedrifter med vikitg data tar ibruk RAID. Dette øker sikkerheten, ytelsen og lagring på serverne. Dersom man kan også ha sitt egen backupserver til hver med formål ved å regenerere hvis noe går galt. Dette kan også bli omtalt som failover system, og øker sikkerheten. Webserveren er banken sin nettside.

Nettverksoppsettet

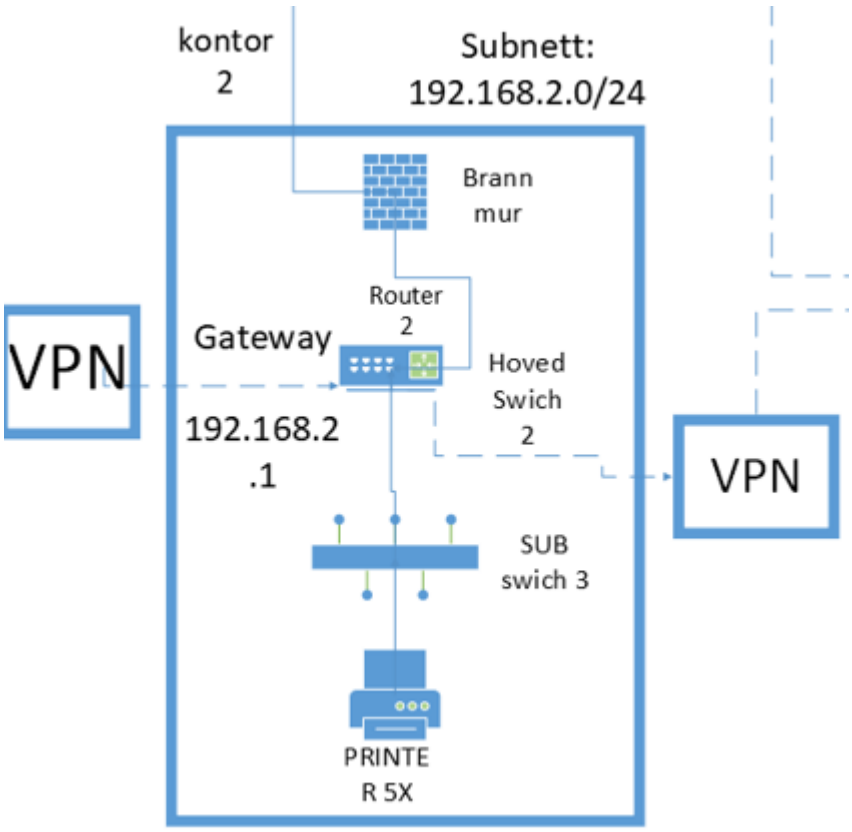
Kontor 1 og Kontor 3





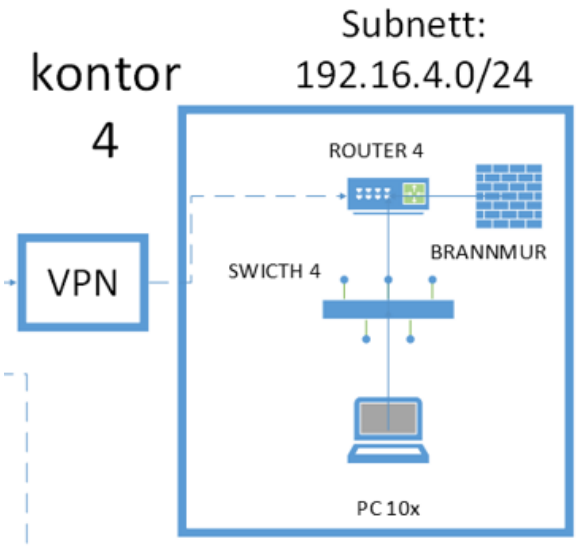
Kontor 1 er hovedkontor og kontor 3 er stort avdelingskontor der det er 50 ansatte hver. De er bygd likt. Det er enheter som printere, pc-er og laptops. 5 enheter per sub switch. Hver sub switch er koblet til en brannmur før hovedswitchen. Den samler pakkene til en router og sender den videre til en brannmur. VPN er også koblet gjennom routeren. Fra brannmuren kobles det til internett. Kontor 1 har en har en adresse 192.168.1.0/24, mens kontor 3 er 192.168.3.0/24.
I kontor 1 og 3 er det mange ansatte så risikoen er større. Det er der hovedkontorene er. Ifølge [1] ChatGPT, 10.03.25, sier de at IT-avdelingen bør ha en egen sub switch bak en ekstra brannmur. Dette vil jeg tro er sant siden om en lekkasje kommer og stopper den på sub switch før hoved switchen.

Kontor 2



Kontor 2 er der rådgivningen skjer. Det er et lite kontor med 10 ansatte. 5 enheter (printere, pc-er og laptops) per sub switch. Samme oppsett som kontor 1 og 3, men ikke brannmur mellom sub switch og hovedswitch. Adressen for subnettet er 192.168.2.0/24.
Jeg har ikke brannmur mellom sub switchene og hovedswitch i kontor 2. I kontor 2 er det fordi det er en relativ lite kontor det er ikke bruk for å bruke ekstra kostnad på en brannmur på et så lite nettverk. Det blir dyrere og kontor 2 er for rådgivning. Derfor holder det med kun en brannmur for datapakkene som blir sent ut til internett.

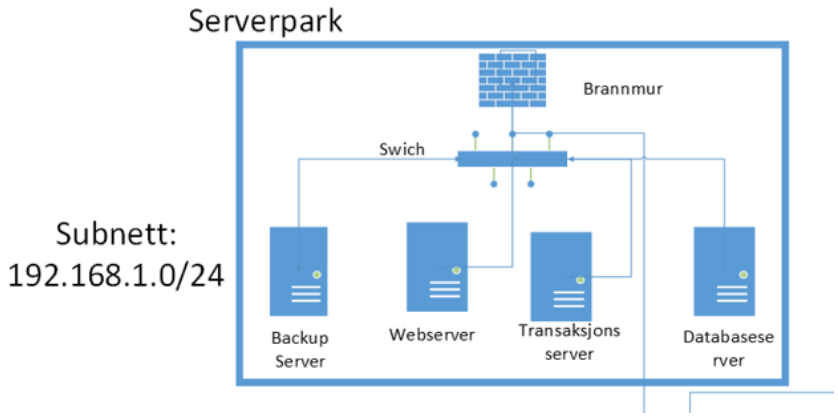
Kontor 4



Kontor 4 er en kritisk avdeling med kun 10 ansatte. Alle enhetene er koblet rett til en Switch, så en router. Routeren kobles med de andre med en VPN. Det har en egen innebygd brannmur for

sikkerheten. Kontor 4 får indirekte tilgang via VPN til de andre kontorene. Dette skjer med en forespørsel. Adressen for subnettet er 192.168.4.0/24.
Kontor 4 er det også en liten kontor og man må tenke på kostnaden. Den egne leide linjen gir nok sikkerhet, det er en egne brannmur ved routeren. Dette skal være sikkert, i kontor 4 er det pengetransaksjonen skjer.

Serverpark



Serverpark er 4 servere som er koblet opp til en switch. Switchen er deretter koblet til en lokal brannmur. Deretter blir den koblet til kontor 1 sin router. Alle ansatte har tilgang gjennom en VPN og brannmur, sånn at kun autoriserte får tilgang. Adressen for subnettet er 192.168.1.0/24. samme som kontor 1 siden de er koblet sammen. Serverparken er koblet til kontor 1 siden den er hovedkontoret mitt, der den blir beskyttet. Serverparken har kundeinformasjon og transaksjonsdata, derfor er det mest fornuftig at den er plassert der.

Sikkerhetsrisikoer og Forbedringer

Dette nettverket er for en bank der jeg har fokusert på sikkerhet. Jeg har subnett som fordeler nettverket for økt sikkerhet. Men nettverket er fortsatt ikke optimalt og det kan gjøres flere forbedringer. Dersom det blir feiloversystem så har jeg en backupserver i serverparken. Jeg kan ikke ta noen sjanser på et angrep eller lekkasje, så må fokusere på
Redundans. Det menes med at jeg har backup på flere komponenter som allerede er der. Flere VPN koblinger og flere brannmurer som støtter de eksisterende er noen tiltak dersom disse svikter. Det er ikke nok sikkerhet i kontor 4. Som sagt skal dette kontoret ha sensitiv informasjon, derfor burde man ha flere sub switcher. VLAN kan bli bruk. Det isolerer trafikken mellom kontorer og servere i nettverket. Som øker sikkerheten. For eksempel kan klientene i VLAN 3 ikke nå databaseserveren i VLAN 1. så en begrenset spredning minker risikoen for angrep. Men det må være VLAN Inter Connect for at VLAN skal vite om hverandre. I switchen kan VLAN gjøre operasjonen mellom pakkene i nettverket eklere for IT å ta hånd om dersom noe skjærer deg. I routeren kan NAT gi en sikkerhet fordi eksterne enheter ser bare bedriftens IP-adresse og ikke dens interne.
For kommunikasjonen kan Subnett forsterke sikkerhetsrisikoen ved å unngå belastning. En annen aspekt man kan gjøre er Load Balancing. Man kan fordele traffiken til serverne i vedlegget. På brannmur bør man øke sikkerheten ved å bruke en DMZ i serverparken for å ha et sikkerhetslag til som logg inn med bankid. Man kan også øke sikkerheten med SPI som er Stateful Packet Inspection. Dette lar kun gyldig datapakker gjennom ved hjelp av forespørsler.
Failover skjer når kritiske komponenter slutter å fungere. Dersom router i hovedkontoret skjer kan dette løses gjennom VPN tunnelene. Der VPN koblingene følger traffikken til et annet kontor. Dersom transaksjonsserveren feiler, kommer backupservern inn.

Konklusjon

Nettverkdesignet er planlagt med tanke på en bank. Der kontor 1 er et hovedkontor, kontor 2 er en liten rådgivning kontor, kontor 3 er et stort kontor og kontor 4 har egne leide linjer med en VPN.

Hvert kontor kommuniserer sikkert med en VPN «tunnel», som krypterer data. Serverparken er koblet til kontor 1 der de andre kontorene må gjennom en brannmur og VPN for tilgang. Alle lokasjoner kan kommunisere med serverparken. Hvert kontor har en lokal brannmur. Kontor 4 bruker leide linjer for ekstra sikkerhet. Alle kontorene kan kommunisere med internett. Det er flere bevisste valg som har blitt tatt. Man kan gjøre nettverket mer sikkert på switchen, router, brannmur og kommunikasjonen. Man må veie seg opp om det er kostnadseffektiv opp mot sikkerheten til banken. Nettverket er satt opp i henhold til OSI- modellen sine lag. Vidre ble det forklar konfigurasjonen av brannvegger og routerne. Hvor IP-adressene/subnettene befinner seg i nettverkdesignet.

Referanser

[1] Hallan Graven., Olaf. Presentasjon 5 *.LAN++.pptx* , USN Universitetet Sør-Øst Norge , (sist besøkt 10.03.2025).

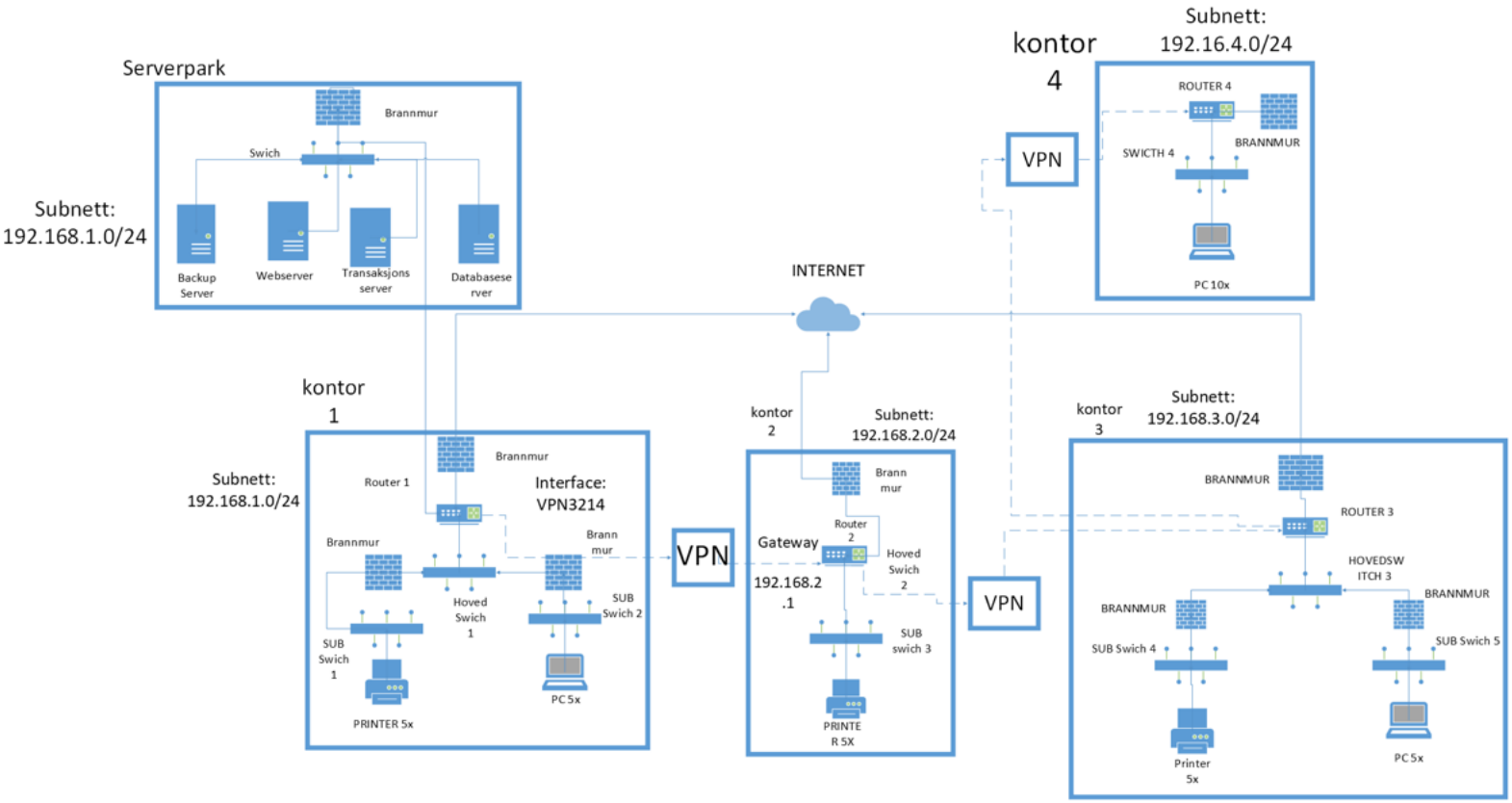
[2] Foldvik Pedersen, Ingar, Presentasjon , *tutorial 10.03.2025.pptx,* USN Universitetet Sør-Øst (sist besøkt 11.03.2025).

[3] ChatGPT , https://chatgpt.com/ (sist besøkt 11.03.2025)

[4] Fortinet, *How Does A VPN Work?* ,https://www.fortinet.com/resources/cyberglossary/howdoes-vpn-work (sist besøkt 03.03.2025)

[5] Hallan Graven., Olaf. Presentasjon 1 *.Intro.pptx* , USN Universitetet Sør-Øst Norge , (sist besøkt 20.03.2025).

Vedlegg


Serverpark
Brannmur
Swich
Subnett:
192.168.1.0/24
Backup Server
Webserver
Transaksjons server
Databasese rver
kontor
4
Subnett:
192.16.4.0/24
VPN
ROUTER 4
BRANNMUR
SWICTH 4
PC 10x
INTERNET
kontor
1
Subnett:
192.168.1.0/24
Brannmur
Router 1
Interface:
VPN3214
Brannmur
Brann mur
Hoved Swich 1
SUB Swich 1
SUB Swich 2
PRINTER 5x
PC 5x
VPN
kontor
2
Subnett:
192.168.2.0/24
Brann mur
Router 2
Gateway
192.168.2 .1
Hoved Swich 2
SUB swich 3
PRINTE R 5X
VPN
kontor
3
Subnett:
192.168.3.0/24
BRANNMUR
ROUTER 3
HOVEDSW ITCH 3
BRANNMUR
BRANNMUR
SUB Swich 4
SUB Swich 5
Printer 5x
PC 5x