Høgskulen på Vestlandet

Bacheloroppgave: BO24EB-07

Fjerntilkobling til feltutstyr i et OT-nettverk

Jørgen Dyrhol Christensen
Lev Elufimov
Leander Surén Levinsen

Cyberfysisk Nettverksteknologi
Fakultet for teknologi, miljø- samfunnsvitskap
Veileder: Adis Hodzic

21.mai 2024

Jeg bekrefter at arbeidet er selvstendig utarbeidet, og at referanser/kildehenvisninger til alle kilder som er brukt i arbeidet er oppgitt, jf. Forskrift om studium og eksamen ved Høgskulen på Vestlandet, § 12-1.

Dokumentkontroll

Rapportens tittel: BO24EB-07 Fjerntilkobling til feltutstyr i et OT-nettverk	*Dato/versjon:* 21. mai 2024 / 1.00
	Rapportnummer: BO24EB-07
Forfatter(e): Jørgen Dyrhol Christensen Lev Elufimov Leander Surén Levinsen	*Studieretning:* CYB21
	Antall sider m/ vedlegg: 58
Høgskolens veileder: Adis Hodzic	*Gradering:* Åpen
Eventuelle merknader: Vi tillater at oppgaven kan publiseres	

Oppdragsgiver: ABB AS	*Oppdragsgivers referanse:*
Oppdragsgivers kontaktperson(er) (inklusiv kontaktinformasjon): *Prosjektveileder:* Erik Serck-Hanssen erik.serck-hanssen@no.abb.com *Faglig veileder:* Nikhil Raj Gupta nikhil-raj.gupta@no.abb.com	

Revisjon	**Dato**	**Status**	**Utført av**
0.01	05.02	Forprosjekt	Jørgen, Lev og Leander
0.02	15.04	2. utgave	Jørgen, Lev og Leander
0.03	18.04	3. utgave	Jørgen, Lev og Leander
0.04	26.04	4. utgave	Jørgen, Lev og Leander
0.05	12.05	5. utgave	Jørgen, Lev og Leander
1.00	21.05	Ferdig rapport	Jørgen, Lev og Leander

Forord

Denne oppgaven er en avsluttende vurdering for bachelor i Cyberfysisk Nettverksteknologi ved Høgskulen på Vestlandet. Rapporten dokumenterer oppgaven «Fjerntilkobling til feltutstyr i et OT-nettverk» som har vært utarbeidet våren 2024 av Jørgen Dyrhol Christensen, Lev Elufimov og Leander Surén Levinsen.

Prosjektet innebærer å utvikle et system av nettverk og servere som skal brukes for å kontrollere et produksjonssystem over Internett. Løsningen på oppgaven er i henhold til ABBs praksis på utvikling av nettverk og kontrollsystemer for å kunne lære og forstå prosjektering i arbeidslivet. Denne metodikken har ført til mange utfordringer og nye temaer underveis, men med god hjelp fra vår faglige veileder har vi kommet i mål med oppgaven. Arbeidet med oppgaven blir sett på som et forberedende eksempelarbeid som nettverksingeniør.

Vi vil takke ABB for å ha gitt oss muligheten til å gjennomføre denne oppgaven. Dette har gitt oss en forståelse for hvordan industrien arbeider innen nettverksteknologi og sikkerhet der gruppen har tilegnet nye kunnskaper innen dette fagfeltet.
Vi vil også takke vår eksterne faglige veileder Nikhil Raj Gupta som har hjulpet oss godt underveis med spørsmål rundt konfigurasjon og design av infrastruktur, og vår interne veileder Adis Hodzic for rådgiving og veiledning til rapportskrivingen.

Sammendrag

Industri 4.0, det digitale automatiseringsskiftet som innebærer tilkobling av eksisterende prosesser og enheter, og utforming av nye systemer som styres over Internett, stiller økt krav til sikkerhet sammenlignet med systemer som ikke er koblet opp mot Internett. Målet med å koble prosesser og systemer til Internett, som et vannkraftanlegg, er å oppnå bedre kontroll og styring, samt øke effektiviteten ved å fjerne behovet for fysisk tilstedeværelse av mannskap. Denne fremgangen åpner muligheten for fjernstyring av offshoreinstallasjoner, for eksempel oljeplattformer, med mindre behov for mannskap på stedet, men heller via kontrollrom på land.

Vår oppgave går ut på å konfigurere et nettverk som kan benytte kontrollsystemer for å drifte og overvåke enheter. ABB har retningslinjer for prosjektering og design av nettverk gjennom standarder som tilfredsstiller spesifikke krav til drift og sikkerhet. Ulike kontrollsystemer har forskjellige krav til drift, sikkerhet og tilgang, og det er derfor avgjørende å sikre at enheter og sensorer kun får tilgang til nødvendig informasjon.

Konfigurasjonen av nettverket og enhetene er i samhold med IEC 62443 og Purdue-modellen. Disse retningslinjene kontrollerer tilgangsnivåer for å gjøre systemer mer brukervennlig for brukere gjennom segmentering og sikring av nettverk. Infrastrukturen er sikret i samsvar med anerkjente standarder. Rapporten viser til fremgangen gruppen har hatt for oppsett og konfigurasjon av et sikkert nettverk.

Innhold

Figurliste

1 Innledning

1.1 Oppdragsgiver

ABB er en ledende aktør innen elektrifisering og automatisering, og fremmer en mer bærekraftig og ressurseffektiv fremtid. Selskapets løsninger kombinerer ingeniørkompetanse med avansert programvare for å optimalisere produksjon, transport, drift og operasjoner. Med rundt 105 000 ansatte og over 130 års erfaring, er ABB forpliktet til å innovere og drive den industrielle omstillingen fremover [1].

ABB har per i dag over 70 millioner tilkoblede enheter hos sine kunder rundt om i verden, som krever innebygde sikkerhetsstandarder. Alt fra kontrollenheter til programvare er designet for å forsikre optimalisert og uavbrutt drift, både gjennom lokaltilkobling og fjerntilkobling. All data til og fra enhetene, samt viktig informasjon, lagres i sikre skytjenester, også levert av ABB [2].

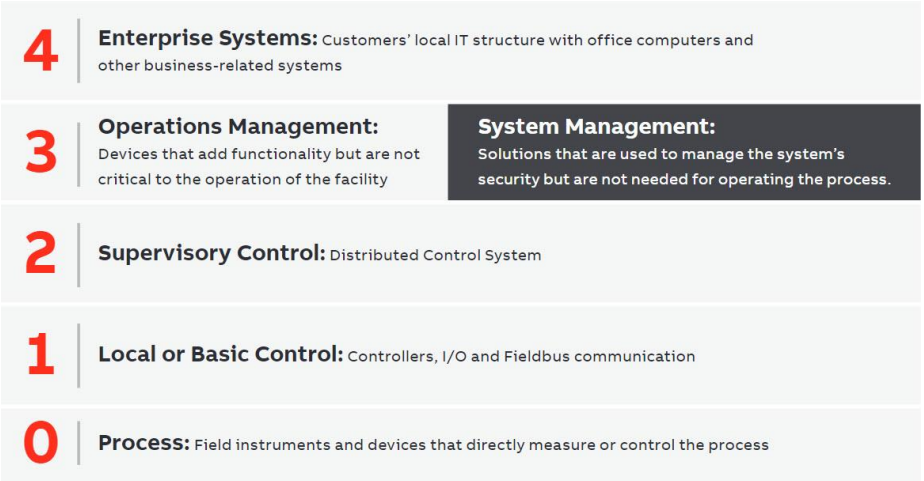
Figur 1: ABBs logo [1]

1.2 Problemstilling

«*Hvordan kan vi sikre fjerntilkobling til et OT-nettverk i samsvar med cybersikkerhetskravene til IEC 62443 og Purdue-modellen?*»

Denne oppgaven går ut på å konfigurere et OT-nettverk for fjerntilkobling til feltutstyrsenheter. Konfigurasjonen skal ivareta cybersikkerhetskravene til IEC 62443 med tilgang på nivå 3 eller høyere i henhold til Purdue-modellen. Det skal også vurderes hvilke cybersikkerhetskrav som er nødvendige for konfigurasjon av brannmurer og switcher for fjerntilkobling mot feltutstyrsenheter.

IEC 62443 er en standard som definerer krav og prosesser for vedlikehold og implementering av elektronisk sikrede industrielle kontrollsystemer gjennom risikoanalyser [3]. Purdue-modellen er en lagvis inndelt referansemodell for design av OT-nettverk for å forsikre at loggføring og adgangskontroll fungerer som tiltenkt, og at systemet forholder seg til bare én bestemt form for tilgang. Oppgaven omhandler konfigurasjon av systemer på lag 3 i Purdue-modellen for å kunne styre fysiske prosesser i de nedre lagene. Som vist i figur 2, fungerer lag 3 som en barriere mellom brukerne i lag 4, og prosessene og kontrollerne i lag 2, 1 og 0. Dermed må lag 3 oppfylle visse krav for å ivareta hele systemets sikkerhet.



Figur 2: Beskrivelse av ABBs implementasjon av Purdue-modellen [21]

Oppgaven krever også fjerntilkobling til ABB sitt testnettverk slik at man er uavhengig av en fysisk tilkobling til det lukkede nettverket. Dette er for å kunne endre på konfigurasjonen på for eksempel en sensor eller motorstyringsenhet i OT-nettverket uten å måtte være fysisk til stede, men også for å få fullverdig tilgang for styring og innsamling av nødvendig informasjon. ABB krever at dette gjøres med en tildelt PC grunnet bedriftens krav for sikker tilgang til deres nettverk.

Konfigurasjon av brannmur og switch krever iverksettelse av nødvendige sikkerhets- og filtreringsmekanismer for å beskytte nettverket mot uautorisert tilgang og potensielle angrep. Dette inkluderer konfigurasjon for å tillate kun godkjent nettverkstrafikk og loggføring av hendelser.

1.3 Analyse av problemet

Systemer som brukes til overvåkning og fjernstyring av enheter bør som standard være godt sikret mot uautorisert adgang. Dette er spesielt viktig i tilfeller ved fjernstyring av aktive feltenheter. Dersom uautoriserte får tilgang for å overvåke eller overstyre enhetene, kan det føre til store problemer for driften av systemet. Risikoen avhenger av hvilke typer enheter som er i drift. For eksempel en skadeovervåningsenhet – denne overvåker statusen på andre enheter i systemet. Dersom en slik enhet blir satt ut av drift gjennom et angrep, kan problemer andre steder i systemet oppstå, alt fra mindre forsinkelser til full systemstans, i følge av angrepet.

Det stilles krav til metode for oppkobling og tilgang for å oppnå ønsket funksjonalitet og drift av systemet for loggføring. Eksempelvis skal all tilgang være fra øvre lag og trinnvis nedover i henhold til Purdue-modellen for at sikkerhetskravene til de ulike lagene skal ivaretas. Dersom dette ikke tas hensyn til, og en lag 4-enhet kobles direkte til en lag 1-enhet, vil ikke hendelsen loggføres korrekt. I tillegg kan sikkerheten til de respektive enhetene bli kompromittert ettersom en slik tilkobling ikke er definert. Dermed kan skadelig data deles mellom disse enhetene, selv om det i utgangspunktet ikke er tillatt.

1.4 Kravspesifikasjon

Kravspesifikasjon gitt fra ABB omhandler at konfigurasjon og fjerntilgang skal ivareta cybersikkerhetskrav med hensyn til ABBs implementasjon av IEC 62443 for utvikling av systemer.

Simple Network Management Protocol version 3 (SNMPv3) skal brukes for å administrere og loggføre trafikk, samt kontrollere adgangskontroll og -nivåer. For at nettverket skal operere på en stabil og sikker måte, må all adgang være gjennom nivå 3 i henhold til Purdue-modellen. Man skal ikke kunne få tilgang til å styre eller konfigurere feltutstyrsenhetene direkte, men via et overordnet kontrollsystem. Nettverket skal segmenteres i adskilte del-nettverk der switch, server og innvendig brannmur skal tillate fjerntilkobling på en sikker måte.
Andre krav er beskrevet i punktene nedenfor.

- Konfigurasjon og hardening av switch og brannmur
- Konfigurasjon av server med virtualisering for installasjon og drift av nødvendig programvare
- Segmentere nettverket i deler for ekstern tilkobling (DMZ), intern administrasjon (Service) og produksjon (A og B)
    - Produksjonsnettverk A og B skal være redundante
- Fjernkobling skal tillates for konfigurasjon og styring av interne enheter.
- All kommunikasjon mellom de segmenterte DMZ-, Service- og produksjons-nettverkene må gå via innvendig brannmur
    - All kommunikasjon mellom innvendig- og utvendig nettverk skal gå via både innvendig og utvendig brannmur
    - Kommunikasjon med utvendig brannmur skal adresseres gjennom NAT

1.5 Hovedidé og utforming av løsning

Det er ulike metoder for å etablere sikker fjerntilkobling mot nettverket, og de ulike alternativene krever ulik konfigurasjon tilpasset hvilket tilkoblingspunkt som blir valgt.
Kravene som stilles til oppkobling og konfigurasjon, er at kommunikasjon innad og utad i nettverket skal være via oversettelse av IP-adresser (NAT).

Etter at alle krav er identifisert, skal dokumentasjon for de forskjellige teknologiene gjennomgås for å forstå konfigurasjon og funksjon. Dette kan inkludere tekniske spesifikasjoner, installasjonsveiledninger og forskjellige sikkerhetsmekanismer. Dette er også med på å tidlig finne ut hvilke deler av oppgaven som kan være mest tidkrevende å gjennomføre. Deretter kan oppsett av nettverket planlegges.

Konfigurasjon og tilkobling av interne nettverk ved adressering og ruting av trafikk vil være lik, uavhengig av hvilken form for fjerntilkobling som blir konfigurert, og hvilken node som er tilkoblingspunkt. Det vil også være noen forskjeller for tilgang og tillatelser for datatrafikk gjennom oppsett av aksesskontrollister (ACL) på brannmuren.
Selve funksjonaliteten, å få tilgang til feltutstyret og styre systemet, vil være den samme uavhengig av hvor tilkoblingspunktet er. Hvordan nettverket er konfigurert vil ikke være synlig for brukeren; ulike løsninger skal kunne gi lik funksjon.

Tilkoblingspunkt i denne oppgaven er forhåndsdeklarert til å være i DMZ-nettverket, dermed må hele nettverket designes slik at DMZ har forbindelse med det eksterne og de interne nettverkene. DMZ sin generelle funksjon er mellomledd mellom Internett og lokalnett. Interne nettverk skal dermed ikke ha forbindelse med utsiden, da dette skal adresseres gjennom DMZ.

Alle enheter konfigureres med hensyn til ønsket tilgang. Det vil si å tillate fjerntilkobling mot enkelte noder, og blokkere fjerntilkobling mot andre noder, og i spesifikke retninger.
Selve fjerntilkoblingen er utstedt av ABB, dermed trenger vi ikke å ta hensyn til den delen av konfigurasjonen, bare legge til rette for at eksterne brukere får tilgang til vårt interne nettverk.

Funksjonen til slike nettverk er en form for å lette drift og administrasjon av produksjonssystemer ved å koble dem til Internett. For at det tilkoblede systemet ikke skal kompromitteres av å være tilgjengelig over Internett, må nettverket også sikre systemet mot eventuelle trusler som kan medføre. Denne oppgaven begrenses til konfigurasjon av enheter på nivå 3 i Purdue-modellen, dermed er sikkerhetskravene som stilles universelle for alle systemer fordi ingen produksjonssystemer, som for eksempel et SCADA-system (*Supervisory Control and Data Aquisition*), er koblet til. Spesifikke sikkerhetskrav for bestemte systemer tas ikke hensyn til, men det skal legges til rette for mulig installasjon av systemer på lag 2, 1 og 0, slik at konfigurasjon skal enkelt kunne endres for å imøtekomme produksjonssystemets sikkerhetskrav.

Det meste av konfigurasjon til switch og brannmur er kjent gjennom tidligere arbeid med switcher, rutere og brannmurer i nettverksfag. Oppsett av server og virtualisering er mindre kjent, dermed vil dette bli en noe mer omfattende prosess. Når hele nettverket og alle systemer er ferdigstilte, skal alle funksjoner testes og analyseres for å vurdere om implementasjonen tilfredsstiller definerte sikkerhetskrav for å avdekke feil eller nye sikkerhetshull.

2 Bakgrunnsteori

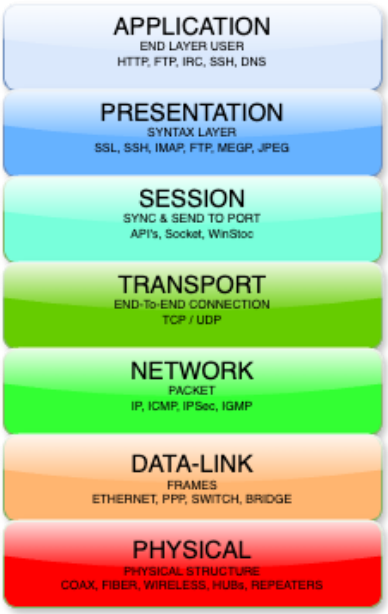
Dette kapittelet beskriver teknologier og terminologier innen nettverksteknologi og -sikkerhet slik at leseren skal kunne forstå arbeidet som er blitt gjort i oppgaven. Dette kan leses i sin helhet eller brukes som referanse.

2.1 Nettverkskommunikasjon

2.1.1 OSI-modellen

OSI-modellen er en mye brukt referansemodell for beskrivelse av ulike teknologier og protokoller i et nettverk. Modellen består av 7 lag der hvert lag er et kommunikasjonspunkt mellom to systemer, hvor hvert lag beskriver spesifikke regler for datakommunikasjon. Dette gir utviklere muligheten til å kunne jobbe på enkelte deler av OSI-modellen [4].
Beskrivelse av de ulike lagene:

7. Applikasjonslaget er det øverste laget som er der brukeren interagerer med grensesnitt mot applikasjoner og andre tjenester.
6. Presentasjonslaget står for kryptering, koding og komprimering av data, og riktig tolking av data for mottakere.
5. Sesjonslaget etablerer og opprettholder økter mellom flere endepunkter.
4. Transportlaget håndterer ende-til-ende leveranse av datapakker, og bekreftelse på mottatte pakker.
3. Nettverkslaget håndterer den logiske adresseringen og rutingen av data, for eksempel ved bruk av IP-adresser.
2. Datalinklaget håndterer overføring av data mellom enheter som er direktekoblet, typisk over samme lokalnettverk.
1. Det fysiske lag definerer fysiske forbindelser og utstyr for overføring av data ved elektriske og/eller optiske signaler.



Figur 3: OSI-modellen

2.1.2 TCP/UDP

Transmission Control Protocol og *User Datagram Protocol* er to viktige transportlagsprotokoller som brukes til å overføre data mellom enheter i et nettverk. Disse utgjør to ulike sett av regler for hvordan trafikk skal håndteres av forskjellige enheter. Selv om de begge brukes til å sende data, har de ulike egenskaper og blir dermed brukt i forskjellige typer nettverkskommunikasjon.

TCP er en forbindelsesorientert protokoll som sikrer ende-til-ende transport av datapakker, og baserer seg på rutingfunksjonalitet fra nettverkslaget (lag 3). TCP tilbyr en pålitelig og sikker måte å sende data ved å ha en aktiv forbindelse mellom server og klient. Dette gjør at tapte pakker vil bli ettersøkt av klient og ettersendt av server.

UDP er en transportprotokoll som er spesielt laget for tjenester der lav forsinkelse er essensielt, som for eksempel Voice over IP-samtaler, videostrømming eller videospill. UDP sender pakkene til mottaker, og senderen vil ikke få noen tilbakemelding på om datapakkene er mottatt eller ikke [5].

2.1.3 Grensesnitt

Definert som et kommunikasjonspunkt mellom to systemer, eller mellom system og bruker. Fysiske grensesnitt kan være ethernet- og seriellporter på switcher, rutere, brannmurer og servere der disse enhetene kobles sammen. For at sammenkoblingen skal godkjennes av begge enhetene, må de operere med samme vilkår og protokoll, definert med portnummer.

Brukergrensesnitt er definert med hvordan en bruker interagerer med en maskin eller programvare for å kunne styre et underordnet system. For administrasjon og tilgang til nettverksenheter, kan brukeren benytte konsollvindu gjennom seriell- eller SSH-tilkobling, eller grafisk gjennom HTTP eller HTTPs, alt etter om enheten støtter grafisk brukergrensesnitt (GUI) eller kun kommandolinje-brukergrensesnitt (CUI).

2.1.4 HTTP og HTTPs

HyperText Transfer Protocol og *HyperText Transfer Protocol Secure* er protokoller som brukes til å overføre data over Internett, eller lokal tilkobling; begge gjennom IP-adresser. HTTP sin hovedbegrensning er mangelen på sikkerhet da data overføres i klartekst. Dette gjør informasjonen sårbar for avlytting og manipulering av tredjeparter. HTTPs legger derimot til et lag av sikkerhet ved å kryptere dataen som overføres mellom webserveren og klienten, samt autentisere tilgang, som gjør det vanskeligere for uautoriserte å avlytte eller endre informasjonen som blir sendt. Protokollene HTTP og HTTPs defineres med portnummer 80 og 443, respektivt.

2.1.5 SSH

Secure Shell er en metode for administratorer å koble seg til andre enheter for tilgang og endre konfigurasjon. SSH kjører via kommandolinje på port 22, og etablerer en kryptert kommunikasjonskanal mellom enhetene, enten koblingen er direkte eller gjennom flere ledd. All data som sendes er konfidensiell, og kan ikke tolkes av uvedkommende.
Dette er en nyere og forbedret versjon av *Telnet* som tillater samme type tilkobling, men all data som sendes til og fra ved bruk av *Telnet* er i klartekst, slik at uvedkommende kan avlytte.

2.1.6 PuTTY og Tera Term

Terminalemuleringsprogrammer av åpen kildekode brukt for å koble til nettverksenheter gjennom seriell, SSH, Telnet eller lignende. Begge programmene støtter ulike protokoller og versjoner, noe som enkelt tillater administrasjon av eldre enheter med utdaterte sikkerhetssertifikater og krypteringsnøkler. Terminalene til oppdaterte versjoner av for eksempel Windows eller MacOS støtter ikke koblinger til utdatert teknologi grunnet sikkerhetshull.

2.1.7 Switch

En nettverksenhet som sammenkobler flere enheter i et LAN. Lag 2-switch er kun for direktekoblede enheter, mens lag 3-switch kan rute trafikk ut av det interne nettverket. En switch opererer vanligvis på lag 2 med MAC-adresser, mens lag 3-switcher støtter ruting med IP-adresser som tillater at enheter kommuniserer på tvers av LAN og VLAN.
Når en ny enhet kobler seg til en switch, vil switchen lagre MAC-adressen i en tabell. Neste gang den MAC-adressen kommer opp i en beslutning, vil switchen kunne slå opp i tabellen og finne hvilket grensesnitt trafikken skal sendes ut av mot riktig mottaker.

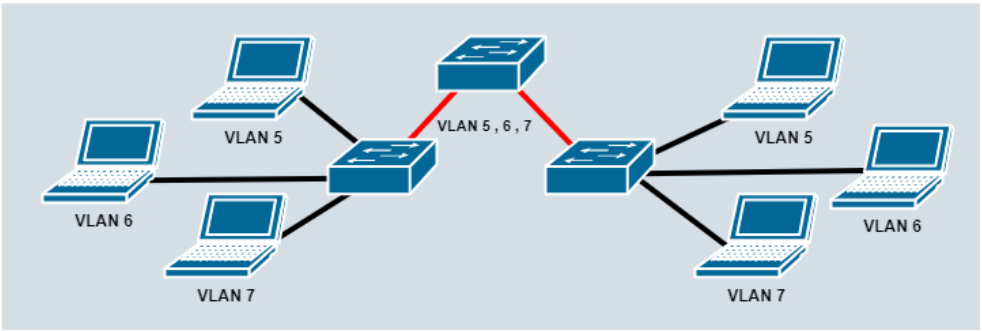
2.1.8 LAN og VLAN

Local Area Network/lokalnettverk er et nettverk som kobler sammen datamaskiner og andre enheter innenfor et geografisk avgrenset område, som et hjemmenett eller et kontornett der deling av ressurser og kommunikasjon tillates. Et LAN er koblet mot et WAN (*Wide Area Network/regionnettverk*) for kommunikasjon med andre LAN, eller over Internett.

Virtual Local Area Network/virtuelt lokalnettverk er en teknologi som brukes for å segregere et LAN i mindre, mer håndterbare delnettverk. Ved å gjøre dette kan brukere være innenfor samme LAN virtuelt, men ikke trenge å være på samme fysiske lokasjon, illustrert i figur 4. Dette kan øke sikkerheten ved å begrense tilgang, og vil i tillegg forenkle administrasjon av enheters plassering og tilkobling i nettverket. Dette gjøres ved å definere hvilke VLAN hvert fysiske grensesnitt tilhører, og trafikk som skal fra et VLAN til et annet vil tagges med VLAN-tag. Data fra et VLAN til et annet kan ikke sendes over Lag 2, men ved bruk av en ruter eller en lag 3-switch, vil dette være mulig.

2.1.9 Trunk- og Access ports

Når man konfigurerer et grensesnitt på en lag 2-switch, kan de konfigureres på to forskjellige måter: *Trunk port*, eller *Access port*. Forskjellen er at *trunk ports* brukes til å sende trafikk mellom enheter i ulike VLAN, og er tilordnet flere VLAN. *Access ports* vil derimot være direkte tilordnet kun ett VLAN, og brukes til å sende trafikk til andre enheter, f.eks. en datamaskin, innenfor samme VLAN. Som illustrert i figur 4, er de røde koblingene *trunk*, mens de svarte er *access*. Figuren viser enheter i ulike VLAN der *trunk*-koblingen tillater kommunikasjon innenfor samme VLAN, selv om de ikke er koblet til samme switch.



Figur 4: Eksempel på VLAN, trunk og access

2.1.10 IT-nettverk

Informasjonsteknologi-nettverk er nettverk der informasjon og ressurser deles og behandles av brukere og enheter som er koblet på det samme lokale nettverket, eller over Internett.

2.1.11 OT-nettverk

Operasjonsteknologi-nettverk er industrielle nettverk som omfatter prosesser med enheter som enten samler inn data i form av målinger, eller enheter og maskiner som gjør bestemte oppgaver, som for eksempel et vannkraftanlegg der man kan styre strømproduksjonen ved å regulere vanntilførsel. I motsetning til et IT-nettverk der data deles og behandles mellom enheter og brukere, er et OT-nettverk for å styre og kontrollere fysiske prosesser, og data herfra sendes til IT-nettverk.

2.1.12 Domene

Et domene representerer et administrativt område i et datasystem eller nettverk. Når det gjelder Internett, refererer et domene eller domenenavn til et unikt navn som tilhører en organisasjon, for eksempel abb.com eller hvl.no. I lokale systemer brukes domener ofte som en betegnelse for sentral administrasjon av brukere eller datamaskiner, som ofte inneholder flere brukere og enheter [6].

2.1.13 Active Directory and Active Directory Domain Services

Active Directory (AD) er en tjeneste fra Microsoft som organiserer og lagrer informasjon i form av objekter innenfor et nettverk. *Active Directory Domain Services* (AD DS) er en av katalogene fra AD, som er integrert i Windows Server. AD DS lagrer dataen ved å bruke en strukturert datalagringsmetode, og sikrer at dataene er lett tilgjengelige for både brukere og nettverksadministratorer. Katalogen inkluderer en rekke ressurser, som ulike typer servere, kontoer og kontogrupper for brukere og datamaskiner på nettverket. Brukerne og gruppene inneholder for eksempel navn, passord og telefonnumre. AD DS har også integrert sikkerhet igjennom påloggingsautentisering og tilgangskontroll til objekter i katalogen. Med en nettverkspålogging kan administratorer håndtere organisasjonen og data i dens nettverk, og autorisere slik at nettverksbrukere kan få tilgang til bestemte ressurser i nettverket. Eksempel på oppgaver og ressurser en administrerende bruker i domenet kan gjøre, er å opprette, redigere og slette brukerkontoer, administrere og implementere gruppepolicyer, overvåke og administrere sikkerhetsrelaterte aspekter, administrere og distribuere programvare- og sikkerhetsoppdateringer til servere i nettverket, sette opp og vedlikeholde tilgangskontroller for filservere og databaser, og konfigurere og overvåke reserveløsninger for å sikre dataintegritet. Dette kan da skje over ulike servere med ulike roller i et domene [7].

2.1.14 Group Policy og Group Policy Objects

Group Policy utgjør en hierarkisk struktur som gjør det mulig for en domeneadministrator å iverksette bestemte konfigurasjoner for både brukere og datamaskiner. Dette systemet brukes hovedsakelig som et sikkerhetsverktøy, og gjør det mulig å påføre sikkerhetsinnstillinger for brukere og datamaskiner [8]. *Microsofts Group Policy Objects* (GPO) er en samling av *Group Policy*-innstillinger som definerer hvordan et system skal fungere for en spesifisert gruppe av brukere [9].

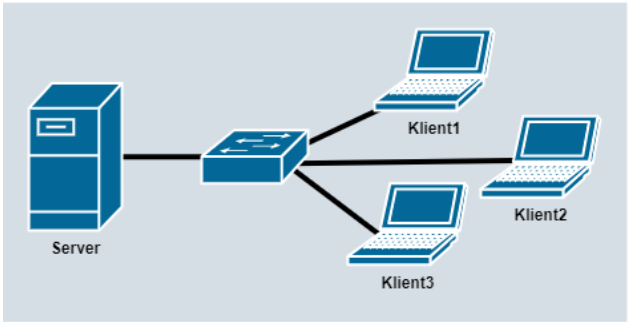
2.1.15 NAT

Network Address Translation er en tjeneste som tillater flere enheter i et privat nettverk å dele en eller flere globale IPv4-adresser for å kommunisere over Internett, ved at den interne private adressen oversettes til en ekstern global adresse. Denne metodikken ble nødvendig grunnet mangel på antall IPv4-adresser i forhold til antall enheter som krever tilgang til Internett.
Typisk vil en abonnent av en Internettjenesteleverandør få tildelt én global IPv4-adresse som alle enhetene på abonnentens hjemmenettverk vil dele for global kommunikasjon.

2.1.16 Host

En host er en enhet som er koblet til et nettverk og kan kommunisere med andre enheter i nettverket. En host kan være både klient og server. Eksempler på host: datamaskin, printer, smarttelefon eller en høyttaler.

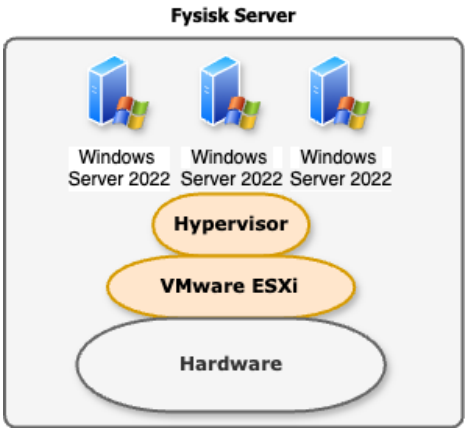
2.1.17 Klient-server-modellen



Figur 5: Klient-server-modellen

En arkitekturmodell som beskriver hvordan forskjellige enheter samhandler i et nettverk for å levere tjenester til hverandre. Klient er for eksempel en PC eller en mobiltelefon som sender forespørsler til en server om å få tilgang til ulike tjenester, ressurser eller informasjon som serveren har tilgjengelig.
Server er en datamaskin som mottar forespørsler fra klienter og tilby etterspurte tjenester, ressurser og informasjon. En server kan håndtere forespørsler fra flere enheter om gangen, som illustrert i figur 5 der en server har forbindelse med tre klienter gjennom en switch. Typisk vil en server håndtere én type tjeneste, dermed har man dedikerte servere for ulike tjenester, for eksempel en for DNS, en for brukertilganger, og en for nettjenester.

2.1.18 Virtualisering



Figur 6: Hierarkisk struktur av virtualisering

Tildeling av ressurser fra en datamaskin for å lage virtuelle maskiner. Én fysisk datamaskin kan segmenteres i flere virtuelle maskiner for bedre utnyttelse av fysiske ressurser, som lagrings-, minne- og prosessorkapasitet, strømforbruk og tilgjengelighet på maskinvare. En bedrift kan trenge flere servere for ulike formål, og ved å bruke én fysisk server segmentert i flere virtuelle servere, vil dette være både ressurs- og kostnadsbesparende for bedriften. Tjenestene som bedriften trenger vil operere på samme måte som om det er tatt i bruk fysiske dedikerte servere; nettverket kan oppfatte at det er flere enheter enn det som fysisk eksisterer, alt etter hvordan nettverket er konfigurert.

2.1.19 Operativsystem

Et operativsystem (OS) er programvare som administrerer maskinvare og gir et grensesnitt for brukere og applikasjoner å samhandle med en datamaskin. OS koordinerer ressursene på datamaskinen, som prosessor, minne, lagring og periferienheter (tastatur, mus, kamera, etc.), og utfører grunnleggende oppgaver som oppstart, styring av filer, og kjøring av programmer. Eksempler på kjente OS er Windows, Linux-distribusjoner, MacOS, Android og iOS.

2.1.20 Hypervisor

Hypervisor er form for programvare eller fastvare som gjør det mulig å skape og administrere virtuelle maskiner. Hypervisoren fungerer som et mellomledd mellom den fysiske maskinvaren (vertsmaskinen) og de virtuelle maskinene.

Type-1 Hypervisor er direkte installasjon på fastvare, et OS som har innebygd funksjonalitet for å opprette og kjøre virtuelle maskiner.

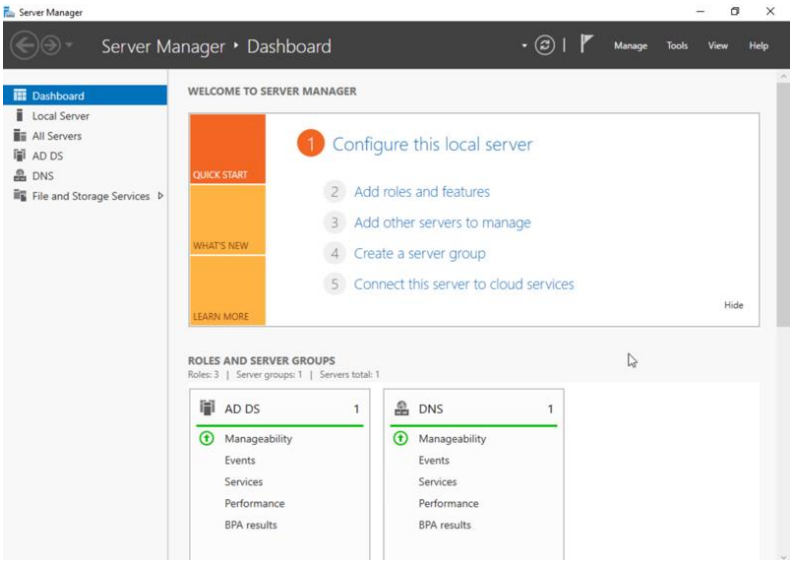
Type-2 Hypervisor er programvare som kjører i et OS, der OS og maskinvare må tillate virtualisering, men type-2-programvaren er ansvarlig for tildeling av ressurser, og håndtering av virtuelle maskiner.

2.1.21 VMware ESXi

VMware ESXi er et OS av type-1 hypervisor i bedriftsklasse som er for å administrere og kjøre virtuelle maskiner. Dette gjør at de virtuelle maskinene blir mer effektive ved å få tildelt flere ressurser, sammenlignet med om de hadde blitt kjørt gjennom en type-2 hypervisor; den fysiske maskinen er mer effektiv og ressurssparende ved at den bruker mindre ressurser på seg selv grunnet OS-ets egne krav til kjøring [10].

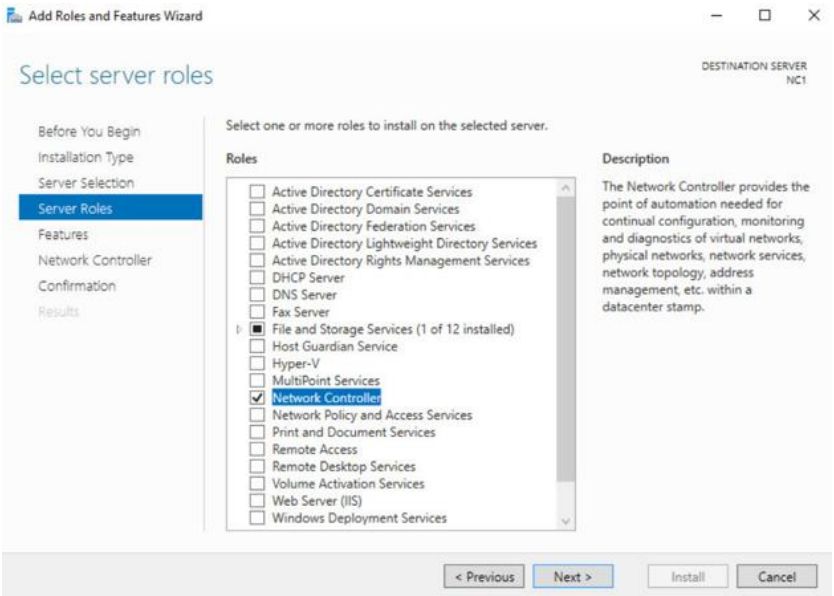
2.1.22 Windows Server

Windows Server er et avansert OS bygget for å levere høyere stabilitet, effektivitet og sikkerhet for servere, enn et OS for klienter. Dette er egenskaper som er kritisk for serverdrift. *Server Manager* er en systemprogramvare som følger med Windows Server, og tilbyr drift for god oversikt over feil og mangler eller sikkerhetshull i nettverket. Dette programmet muliggjør konfigurasjonen av serveren for å håndtere bestemte roller, som understreker OS-ets fleksibilitet og tilpasningsevne til ulike server-roller.



Figur 7: Windows Server Manager

En *server-rolle* definerer funksjonene og ansvarsområdene en server har innenfor en nettverksinfrastruktur, mens egenskaper (features, figur 8) er valgfrie programvarekomponenter som kan installeres for å forbedre serverens kapasitet [11]. Figur 8 illustrerer noen av de ulike server-rollene man kan installere på *Server manager,* for eksempel kan det installeres *AD DS* og *Domain name Server (DNS)* ved hjelp av *add roles*-verktøyet.



Figur 8: Meny i Windows Server for valg av serverroller

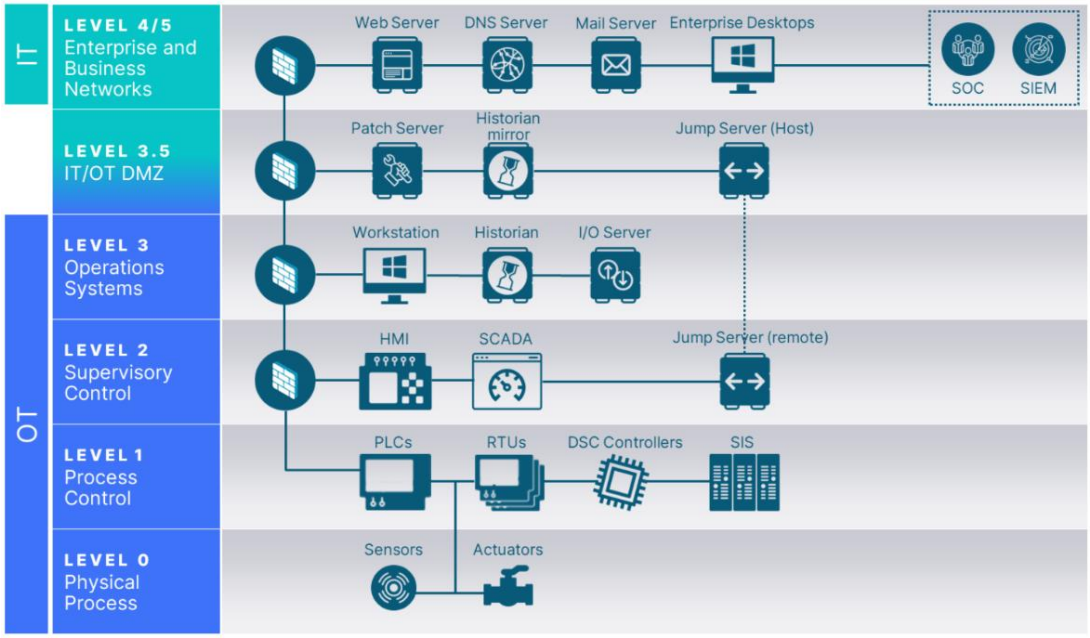
2.1.23 RDP

Remote Desktop Protocol er en proprietær kommunikasjonsprotokoll utviklet av Microsoft som tillater fjerntilkobling mot en Windows server gjennom port 3389 med et grafisk brukergrensesnitt. Brukeren får tilgang til enhetens skrivebord fra sin lokale maskin, og kan overstyre serveren uten å fysisk kontrollere serveren [12].

2.2 Nettverksikkerhet

2.2.1 Purdue-modellen

En standardisert modell for design, organisering og segmentering av nettverk i flere nivåer for ulik tilgang og bedre kontroll.



Figur 9: Eksempel på Purdue-modellen [18]

Lag 4/5: Området der brukere og ressurser befinner seg; nettverket som er koblet til Internett.
lag 3.5: Sone som ivaretar sikkerhetskravene til lagene over og under for sikker kommunikasjon mellom dem. Fjerntilkobling til lavere lag skjer gjennom lag 3.5. Her finnes også prosessene som overvåker og loggfører hendelser i de nedre lagene.
Lag 3: Driftsområdet der overvåknings- og styringsmaskinene for de fysiske prosessene befinner seg. Tilgang til systemene som er i drift, de fysiske maskinene i lavere lag, er gjennom serverne i lag 3.
Lag 2: Kontrollsystemene for styring av de fysiske prosessene. Her for eksempel SCADA-system som har tilgang til alle SCADA-ressurser, og er grensesnittet for kontrollerne til de fysiske enhetene, som for eksempel en sensor eller en turbin.
Lag 1: Kontrollerne som mottar data fra de overordnende grensesnittene og styrer de fysiske prosessene til enhetene.
Lag 0: De fysiske enhetene som driftes, mottar hendelsesdata fra kontrollerne og sender driftsdata.

Konsekvensene av å ikke bruke en lagdelt modell for operasjonsnettverk, vil være uregelmessig eller manglende loggføring av hendelser, spesielt med hensyn til regulering av enheter, som for eksempel turbiner. Ved å designe nettverket i samsvar med Purdue-modellen, vil alle prosesser bli administrert fra servere på lag 3. Data vil bli sendt opp og ned gjennom lagene i nettverket, samtidig som sikkerhetsaspekter ved de ulike systemene ivaretas.
For eksempel, dersom en lag 4-enhet, en bedriftsdatamaskin med Internettilgang, kobles direkte til en turbin i lag 0, vil ikke sikkerheten til enhetene ivaretas. Dette kan føre til spredning av skadelig programvare fra lag 4 ned til lavere lag, og slike hendelser vil ikke bli loggført siden de ikke går gjennom kontrollsystemene. Systemet på lag 2 og lag 3 vil oppfatte den endrede konfigurasjonen som en uregelmessig hendelse.

2.2.2 IEC 62443

En sikkerhetsstandard for cybersikkerhet og drift i automasjon- og kontrollsystemer for å beskytte systemer mot eventuelle trusler og svakheter [3]. Denne standarden er et rammeverk for design av nettverk ved å kartlegge sikkerhetskrav og sikkerhetsnivåer, samt risikoer.
IEC 62443 definerer 4 sikkerhetsnivåer, der nivå 1 er lavest, og nivå 4 er høyest. Typisk for nivå 1 vil være systemer med ingen til få tilkoblinger mot andre systemer, der andre systemer har ingen til begrenset avhengighet til systemets funksjoner, for eksempel et hjemmenettverk. Typisk for nivå 4 er systemer med ressurser som er kritiske for andre systemers funksjon, for eksempel banksystemer, dermed er det høyere krav til sikkerhet enn lavere nivåer.
Standarden er også definert i ulike kategorier: 62443-1 til 62443-4. Denne oppgaven er i henhold til spesifikasjonene for 62443-3 og dens underkategorier, 3-1 til 3-3.
62443-3-1 gjelder for *industrielle automasjons- og kontrollsystemer* (IACS) ved bruk av ulike sikkerhetsteknologier. 62443-3-2 er design av system og risikoanalyse, og 62443-3-3 er videre design av system gjennom sikkerhetskrav og sikkerhetsnivåer [13].

Risikovurdering er å identifisere eiendeler, ressurser, trusler, svakheter, skadeomfang og sannsynlighet for skader. Etter gjennomført risikovurdering, må man iverksette mottiltak for å hindre eller minske risikoer som ble avdekket. Sikkerhetskrav er design gjennom retningslinjer til hva bedriften setter som krav til systemet. Det kan være å segmentere nettverket i ulike deler for ulike bruksområder, sikre lokale og eksterne kommunikasjonskanaler, redundans og reserveomkobling for å redusere nedetid dersom hovedsystemet skulle svikte. Alle sikkerhetstiltak må også adresseres gjennom hele systemets levetid gjennom forbedringer og oppdateringer etter nye krav og scenarioer, definert etter hvor lenge systemet trenger å være i drift.

2.2.3 VPN

Virtual Private Network er en måte for private nettverk å kommunisere og sammenkobles over usikret nett, som Internett, ved at man etablerer logiske kommunikasjonskanaler mellom nettverk.

Site-to-site VPN er typisk for virksomheter som har lokasjoner på flere steder. Dette er en metode for å sammenkoble hele virksomhetens nett over Internett gjennom sikre kommunikasjonskanaler. Bruk av VPN eliminerer behovet for private fysiske koblinger mellom lokasjoner.

Remote Access VPN er for enkeltbrukere av en virksomhet, eller annet vilkårlig privat nettverk, der man kan få tilgang til det private nettverket over usikret Internett. Dette er typisk en løsning for hjemmekontor, ved at enkeltbrukere er koblet til bedriftens nett og har tilgang til bedriftens ressurser, selv om man ikke er fysisk til stede.

2.2.4 SNMPv3

Simple Network Management Protocol version 3 er en protokoll som aktiveres på enheter i nettverket for å loggføre statusinformasjon og hendelser. Det er en måte å overvåke nettverket, som gjør det lettere for driftsansvarlige å feilsøke og kunne forstå nettverkets drift.
Versjon 3 har støtte for kryptering og autentisering av SNMP-trafikk og -brukere. Dette kan øke sikkerheten til nettverket ved at kun autentiserte brukere har tilgang til enheters statusinformasjon.

2.2.5 Brannmur

En nettverkssikkerhetsenhet som overvåker innkommende og utgående trafikk, og tillater eller blokkerer datatrafikk basert på konfigurerte regler ved angitte protokoller og porter på lag 3.
En brannmur fungerer som en barriere mellom interne lokalnettverk og utvendige nettverk, som Internett.

2.2.6 ACL

Access-Control List er hvor man definerer regler for å tillate og nekte datatrafikk basert på avsender, mottaker, og protokoll eller datatype ved bruk av lister. Det er en form for å kontrollere adgang ved å tillate bestemte funksjoner, og nekte uønsket trafikk; både for å sikre nettverket for uønsket trafikk, men også for å redusere overhead ved å forkaste unødvendig trafikk.
Eksempel:

```
1: permit any any eq https
2: deny any any
```

Denne rekkefølgen tillater HTTPs-trafikk fra alle kilder mot alle kilder, og blokkerer alt annet.

```
1: deny any any
2: permit any any eq https
```

Her vil all trafikk blokkeres selv om HTTPs-trafikk er tillatt; det er den første linjen som gjelder. Siden tillat kommer etter nekt, og linjen for å nekte matcher samme avsender og mottaker som linjen under for å tillate, vil linje 2 aldri bli tatt i bruk.

2.2.7 DMZ

Demilitarized Zone er et isolert område fra det eksterne og interne nettverket. DMZ fungerer som et bufferområde mellom den interne delen av nettverket som inneholder sensitive systemer, og den eksterne delen som kan være farlig eller skadelig for det interne nettverket. Formålet til DMZ er å styrke nettverket ved å begrense tilgangen fra eksterne kilder. Dette gjøres ved å bruke brannmur og andre sikkerhetsmekanismer for å isolere og begrense trafikken mellom områdene.

2.2.8 Portsikkerhet

Metodikk for å sikre fysiske nettverksporter ved å deaktivere funksjoner som ikke er nødvendige for nettverkets drift. Typisk ved å skru av alle ubrukte porter, slik at nye tilkoblinger ikke vil være aktive; ingen trafikk sendes eller mottas. Andre tiltak kan være å begrense antall koblinger pr port, med antall registrerte MAC-adresser, typisk ved kobling til andre switcher, og kun tillate og aktivere nødvendige protokoller og portnumre.

2.2.9 TLS/SSL

Transport Layer Security/Secure Socket Layer er protokoller på applikasjonslaget i OSI-modellen som krypterer kommunikasjon over nettverk, mest brukt med HTTPs, ved bruk av sertifikater mellom klienter for autentisering. *TLS 1.0* ble introdusert i 1999 og oppdatert til *TLS 1.3* i 2018; en oppdatert versjon av *SSL*, introdusert i 1994 [14].

2.2.10 KeePass

En passordbehandler med åpen kildekode, som gjør det enklere å generere, håndtere og lagre passord på en sikker måte. For eksempel en person som har brukere på forskjellige nettsider, og siden god sikkerhetspraksis er unike og sterke passord, vil det være vanskelig å memorere alle passordene. Alle passord lagres i en database som er beskyttet av et masterpassord som gir tilgang til alle passord. Databasen er kryptert med en avansert og sikker krypteringsalgoritme, for eksempel AES 256 [15].

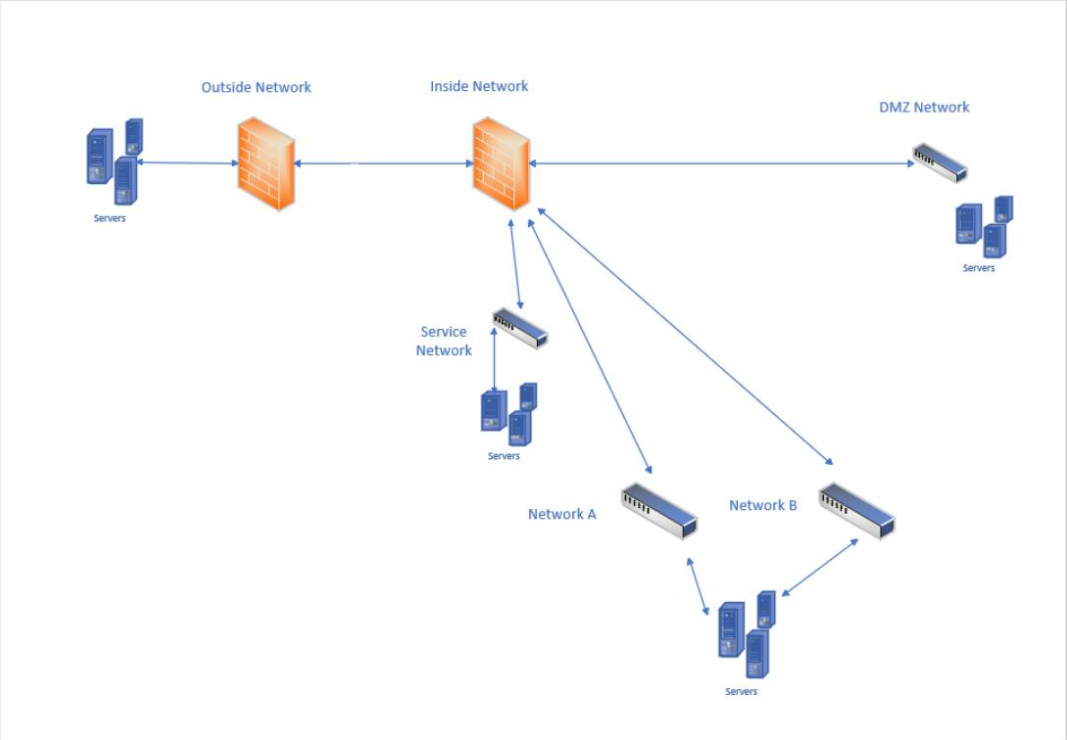
3 Realisering av løsning

Dette kapittelet forklarer hvordan vi utførte løsningen, etterfulgt av designet og strukturen av nettverket. Delkapittel 3.3 til 3.6 er delt opp i flere delkapittel hvor de forskjellige enhetene forklares, etterfulgt av konfigurasjon.

3.1 Fremgangsmåte

Vi startet med å kartlegge oppgaven gjennom møter med både ekstern og faglig veileder for å tydeliggjøre og begrense oppgavens krav, og avklare fremgangsmåte for oppgavegjennomføringen.

Oppgavebeskrivelsen inneholdt denne skissen av nettverket (figur 10), som er en enkel logisk modell som ikke samsvarer med den fysiske infrastrukturen til det interne nettverket. Vi arbeider kun med én fysisk server og én fysisk switch, og ikke 4 switcher og 3 servere. Både serveren og switchen segmenteres i ulike logiske virtuelle deler som plasseres i sine respektive virtuelle nettverk. Dette er både grunnet begrenset tilgang til fysiske enheter, men også design av infrastruktur i henhold til standardpraksis i operasjonelle nettverk.

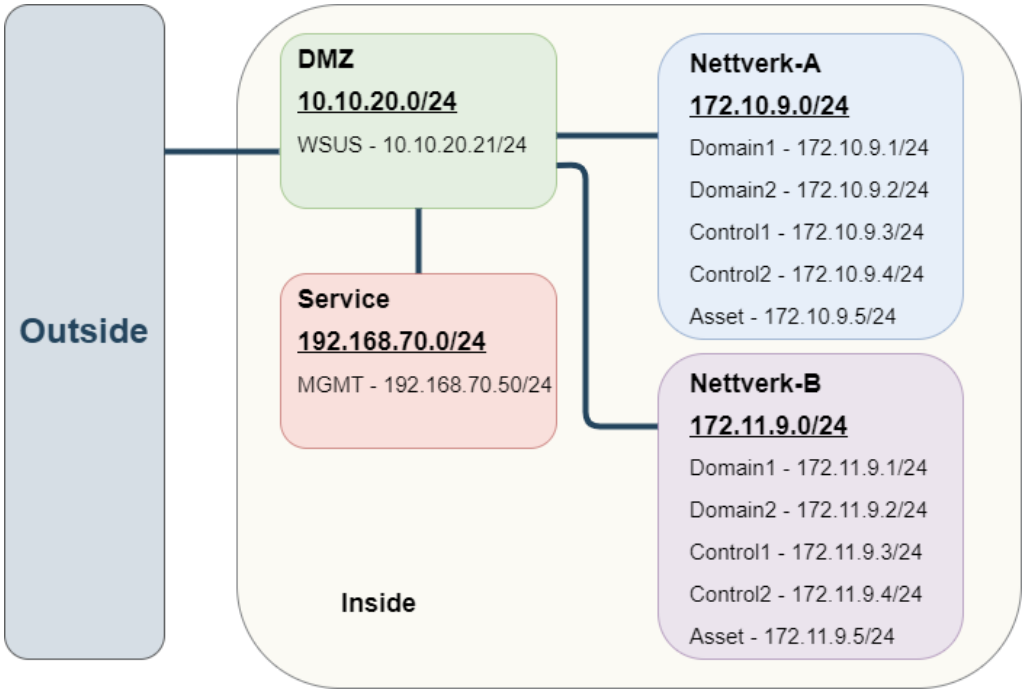


Figur 10: ABBs skisse av OT-nettverket

Realiseringen av nettverket som beskrevet, bydde på utfordringer spesielt knyttet til å ha servere som opererte i to nettverk, samtidig som all kommunikasjon fungerte feilfritt. Brannmuren har kun 4 fysiske porter, og det kreves 5 tilkoblinger, dermed måtte minst to av nettverkene dele samme fysisk port, noe som kan motarbeide kravet til redundans.

For redundans av Nettverk-A og -B, ble disse tildelt egne porter, mens DMZ- og Service-Nettverket deler samme fysisk port ved å segmentere porten i to logiske porter tilhørende deres respektive VLAN. Porten for tilkobling mot utsiden, den eksterne brannmuren, er også tildelt egen fysisk port.

Denne løsningen ble valgt med tanke på drifts- og sikkerhetskrav, der DMZ- og Service-nettverkene sender mindre trafikk sammenlignet med Nettverk-A og -B, og Utsiden når fjerntilkobling er aktiv. Det må også merkes at overføringshastigheten til brannmurens porter er lav (100mb/s) sammenlignet med dagens «vanlige minstekrav» (1000mb/s), noe som kan resultere i flaskehalser dersom flere nettverk deler samme port.
Figur 11 viser en logisk oversikt av det interne nettverket med alle serverne som befinner seg i de ulike del-nettverkene. Her ser man at Nettverk-A og -B inneholder samme servere.



Figur 11: Topologi av hele nettverket

Før oppstart av det fysiske arbeidet måtte vi vente på å få utlevert utstyr fra ABB. Dette ble noe forsinket fra ABB sin side, grunnet at dem ikke hadde en server tilgjengelig i Bergen og det måtte tilsendes en fra Stord. Det ble også noen forsinkelser med den utlånte PC-en, på grunn av problemer med ABB sine sertifikater og sikkerhetsrutiner som er satt rundt utlån av utstyr.
Denne PC-en skulle opprinnelig brukes til å konfigurere nettverket, men dette var ikke mulig da man trenger administratortillatelse for å kunne bytte IP-adresse for å få tilgang til enhetene. Derfor har vi brukt våre private PC-er for konfigurasjon, og den utlånte PC-en ble kun brukt for tilgang via VPN.

Etter at alt utstyret var tildelt, koblet vi det opp og sjekket at hver enhet fungerte, først hver for seg og dermed sammenkoblet. Videre planla vi nøye hvordan enhetene skulle kobles opp og utførte tester ved bruk av ping for å sikre korrekt oppkobling og kommunikasjon mellom enhetene.

I løpet av forprosjektfasen planla vi å undersøke all bakgrunnsinformasjon, som protokoller og brukerdokumentasjon, slik at vi var godt forberedt til å konfigurere nettverket så fort vi fikk tilgang til utstyret. Dette viste seg etter hvert å være utfordrende grunnet uklarhet av hvilke produsenter enhetene vi ville få var fra, og hvordan OT-nettverk fungerer, samt tydeliggjøring av oppgavens rammer. Dermed måtte vi planlegge og innhente bakgrunnsinformasjon underveis i prosjektet, noe som førte til en del forsinkelser i forhold til vår opprinnelige tidsplan. Til tross for dette var prosjektet planlagt med gode marginer, så disse forsinkelsene var ikke et betydelig hinder for oppgaven.

3.2 Design og struktur

Etter at enhetene var testet, startet vi å konfigurere hver enhet separat. Serveren var det første vi satt opp ved å installere *VMware ESXi* med 7 virtuelle maskiner med *Windows Server 2022*. Disse virtuelle maskinene skulle ha forskjellige roller i nettverket: *Domain1-Server*, *Domain2-Server (secondaryDomain)*, *Management-Server*, *Asset-Server*, *Control-Server* og *WSUS-Server*. Først installerte vi konsollversjonen, *Core*, (figur 12) av Windows Server 2022 i stedet for den grafiske skrivebordsversjonen (figur 13), som er normalt å installere. Dette ville gjort oppgaven mer kompleks enn nødvendig ved å måtte jobbe i kommandovindu uten umiddelbar kjennskap til kommandoer.

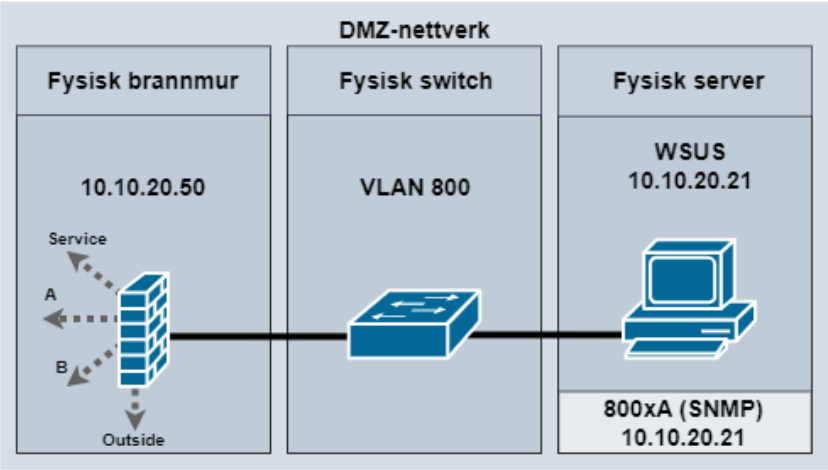
Vi installerte først Core-versjonen fordi den grafiske versjonen krever flere ressurser sammenlignet med for eksempel en distribusjon av en grafisk Linux server. Vi regnet med at den fysiske serveren ikke hadde tilstrekkelig lagrings- og prosessorkapasitet til å håndtere 7 grafiske Windows-servere. Etter videre undersøkelser og dialog med faglig veileder, som fortalte oss at det ikke ville være problematisk med grafisk Windows server, valgte vi dermed å installere alle serverne på nytt med skrivebordsversjonen.

Figur 12: Server uten skrivebordsmiljø

Figur 13: Server med skrivebordsmiljø

For meningsfull rollefordeling blant serverne og muliggjøre kommunikasjon mellom dem, samtidig som annen kommunikasjon begrenses, må nettverket segmenteres i ulike deler. Dette tilfredsstiller også sikkerhetskrav for isolering av enheter og grensesnitt ved å dele opp nettverket.

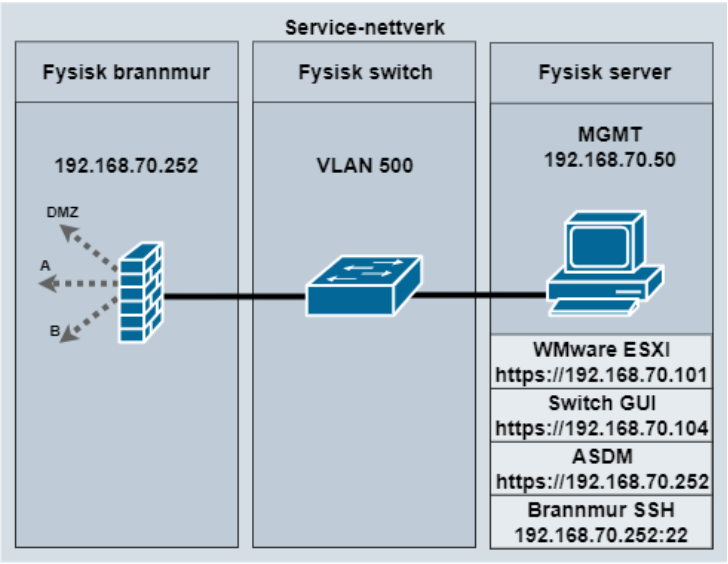
DMZ-nettverket (figur 14) inneholder WSUS-Serveren. Dette nettverket fungerer som et mellomledd mellom det interne og det eksterne nettverket, og er porten inn for ekstern tilgang til det interne nettverket, som tilsier nivå 3.5 i Purdue-modellen. Dette vil si at all tilgang som skal til den fysiske serveren, og administrasjon av de virtuelle maskinene, må skje gjennom denne delen av nettverket. WSUS-Serveren sin hovedoppgave er å hente Windows-oppdateringer og tildele dem til de andre serverne i nettverket. Det er derfor viktig at den er i DMZ, et område som har tilgang til både det eksterne og interne nettverket.



Figur 14: Topologi av DMZ-nettverket

WSUS-serveren fungerer også som SNMP-serveren, der alle hendelser loggføres, og en administrator kan hente ut informasjon for eventuell feilsøking. Programvaren som skal brukes er ABBs 800xA for å loggføre SNMP-hendelser og annen nettverksstyring. Denne programvaren brukes også for styring av prosessene i lag 2, 1 og 0 i henhold til Purdue-modellen, da feltenhetene som er konfigurert for styring og bruk gjennom 800xA, er også konfigurert for å sende SNMP-meldinger ved bruk av samme programvare for sentralisert administrasjon.

Service-nettverket (figur 15) er på nivå 3 i Purdue-modellen, og inneholder Management-serveren som har tilgang til VMware ESXi, og kan endre konfigurasjon til alle de andre serverne i hele nettverket. Selv om Management-server kan få tilgang til alle de andre serverne gjennom ESXi, er ikke dette riktig tilgangsmåte grunnet at denne type tilgang skjer lokalt på den fysiske serveren, og er ikke adressert gjennom nettverket. Dette vil kunne skape problemer for adgangskontroll og loggføring av hendelser, fordi brannmuren og nettverket er ikke involvert i denne kommunikasjonen.

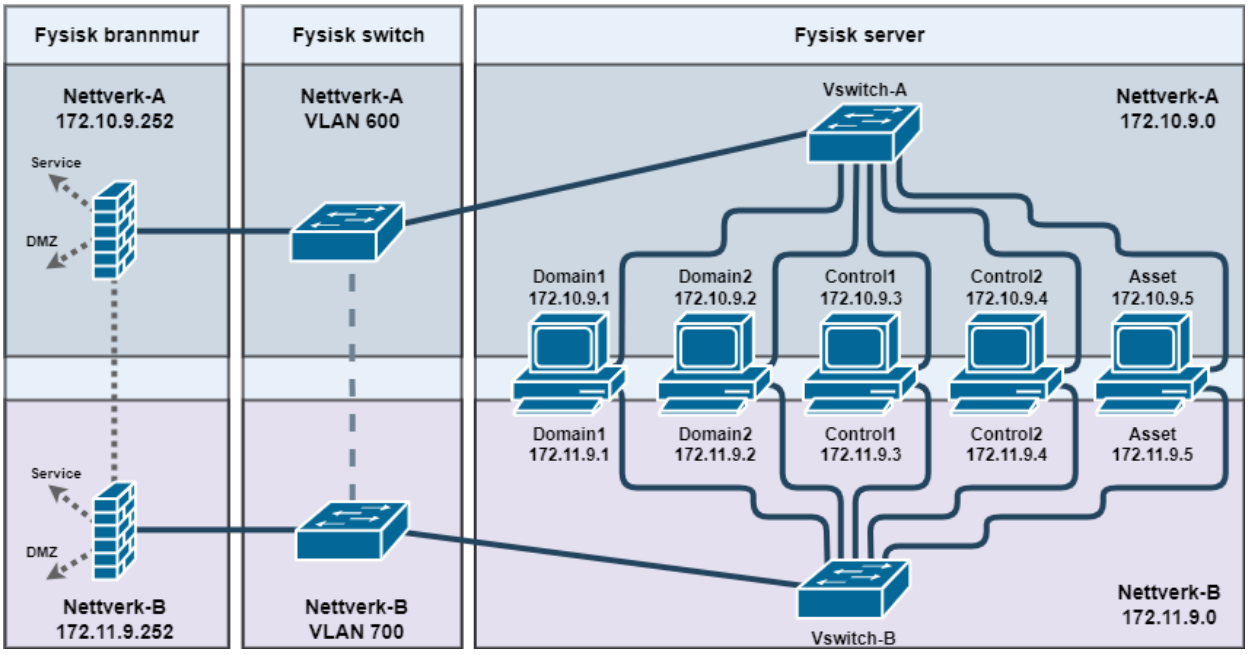


Figur 15: Topologi av Service-nettverk

For å tilfredsstille kravene til Purdue-modellen og IEC 62443 for ønsket adgangsform, må adgang til ESXi kunne reguleres i form av korrekt loggføring ved bruk. Denne type tilgang må også kunne begrenses til kun autorisert personell som kan være adskilt fra annet personell som skal ha tilgang til for eksempel kun Nettverk-A og B; Service og DMZ ekskludert.

Management-serveren har også administrasjonstilgang til både switchen og brannmuren. Ved opprinnelig konfigurasjon av nettverket ble våre private datamaskiner brukt til å få tilgang til både switchen og brannmuren. Når nettverket er ferdigkonfigurert, vil den eneste måten å få tilgang på være via VPN til DMZ-nettverket, og videre gjennom Management-serveren for å se og endre konfigurasjonen; alle andre fysiske porter og tilganger vil være deaktivert. Alle aktive grensesnitt (SSH og HTTPs) til enhetene er plassert i Service-nettverket som vist i figur 16.

Nettverk-A og Nettverk-B (figur 16), er to nettverk med lik funksjonalitet som er på nivå 3 i Purdue-modellen. Alle operasjonsserverne, dvs. alle serverne som er tiltenkt å kjøre systemer for drift av industrielle systemer på lag 2, 1 og 0 i henhold til Purdue-modellen, er plassert i både Nettverk-A og Nettverk-B. Nettverk-B fungerer som et reservenettverk dersom nettverk-A går ned, derfor tar man i bruk to eller flere nettverk for å tilfredsstille kravet til nær 100% oppetid. Nettverk-A og Nettverk-B vil kunne ha prosesser som kjører 24/7, mens DMZ og Service sine tjenester er kun i bruk ved behov, dermed stilles det ikke krav til nær 100% oppetid for disse nettverkene.



Figur 16: Topologi av nettverk-A og -B

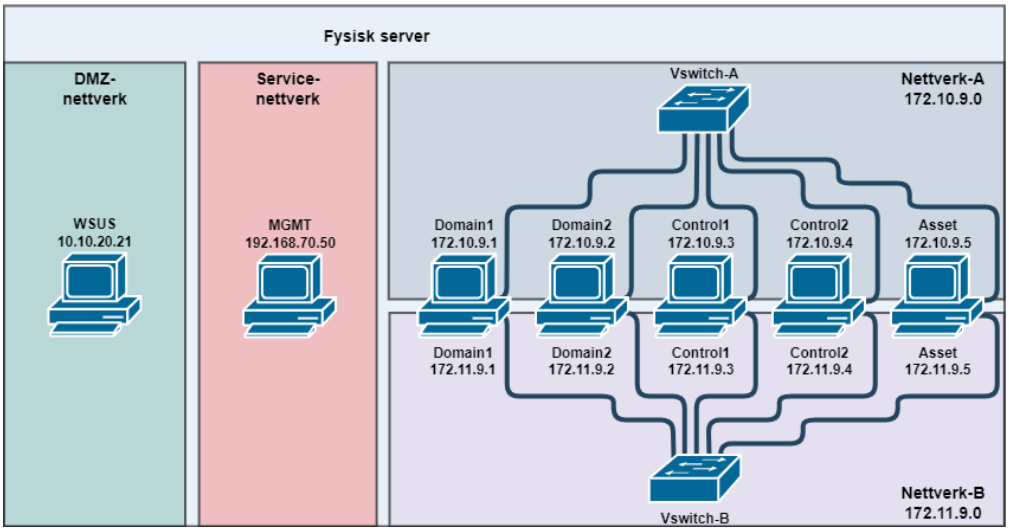
3.3 Server

Dette kapittelet omhandler serverinfrastrukturen og dens konfigurasjon. Først forklares den fysiske serveren og operativsystemet. Deretter vil domenet og dets administrative funksjoner forklares, og så rollene og funksjonene til de ulike virtuelle serverne hver for seg.

3.3.1 Utstyr og operativsystem

Serveren som ble tatt i bruk er en Dell E45S fra 2017, og er utstyrt med fire 600GB harddisker, en 16 kjerners CPU, 32GB RAM og to strømforsyninger for redundans; i tilfelle den ene strømforsyningen svikter, vil serveren fortsatt være i drift. Kun to av de fire diskene er i drift i en RAID 1-konfigurasjon, noe som gir totalt 600GB lagringsplass da diskene er speilet. Disse innstillingene er standard, og vi har ikke endret konfigurasjonen av diskene da det ikke er nødvendig for gjennomføringen av denne oppgaven. Serverne i dette nettverket er kun konfigurert for å være tilkoblet domenet og være påslått, derfor er 7 servere fordelt på 2 disker tilstrekkelig i dette scenarioet. Likevel er RAID 1 en god praksis siden den gir redundans; hvis en disk feiler, vil ikke data gå tapt, i motsetning til RAID 0 der alle diskene blir lagt sammen for å øke lagringskapasiteten.
ABB lisensierte installasjon av OS. Den fysiske serveren kjører VMware ESXi 7.0, og de virtuelle maskinene kjører Windows Server 2022; Begge versjonene støttes fortsatt av produsent, i motsetning til fysisk utstyr.

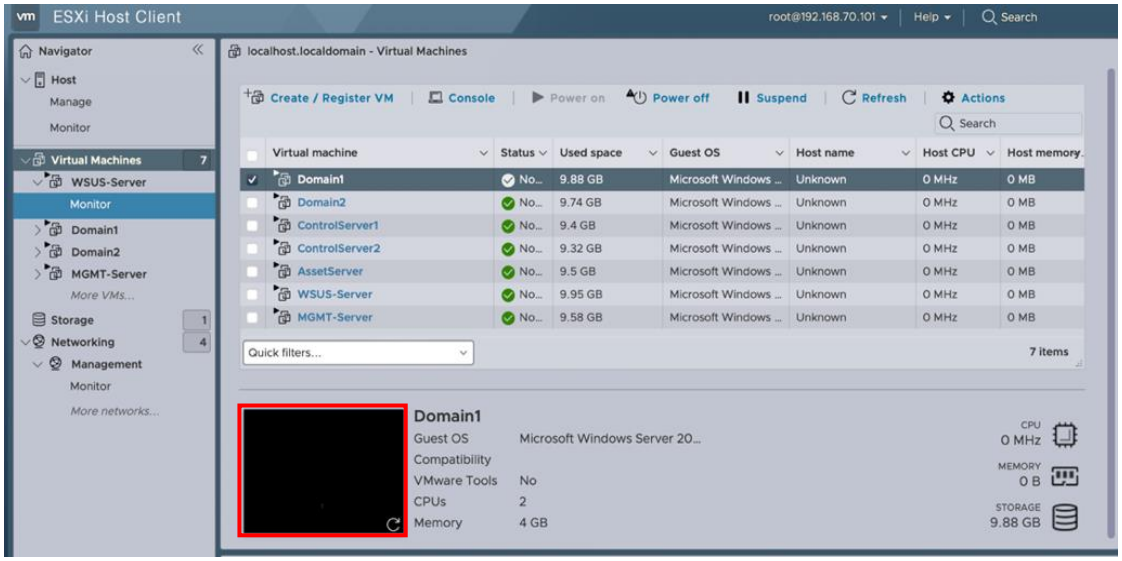
VMware ESXi har innebygde virtualiseringsfunksjoner, og kjører alle de 7 virtuelle maskinene som illustrert i figur 17. I henhold til denne oppgaven, og ABBs praksis, er det ingen begrensinger til bruk i form av Legacy-systemer knyttet til nyeste versjon av Windows server.



Figur 17: Den fysiske serverens interne nettverkstopologi

Etter installasjon av OS, var neste steg å etablere en metode for administrasjon og kontroll av den fysiske serveren. Dette var gjennom tilordning av en IP-adresse, 192.168.70.101, for administrasjonstilgang. Figur 18 viser det grafiske brukergrensesnittet for administrasjon av VMware ESXi. Gjennom det grafiske brukergrensesnittet er det konfigurert virtuelle maskiner med spesifikasjoner for tildelt minne, lagring og prosessorkjerner. Hver av de virtuelle maskinene er tildelt to prosessorkjerner, 4GB minne og opptil 90GB dynamisk allokert lagringsplass.

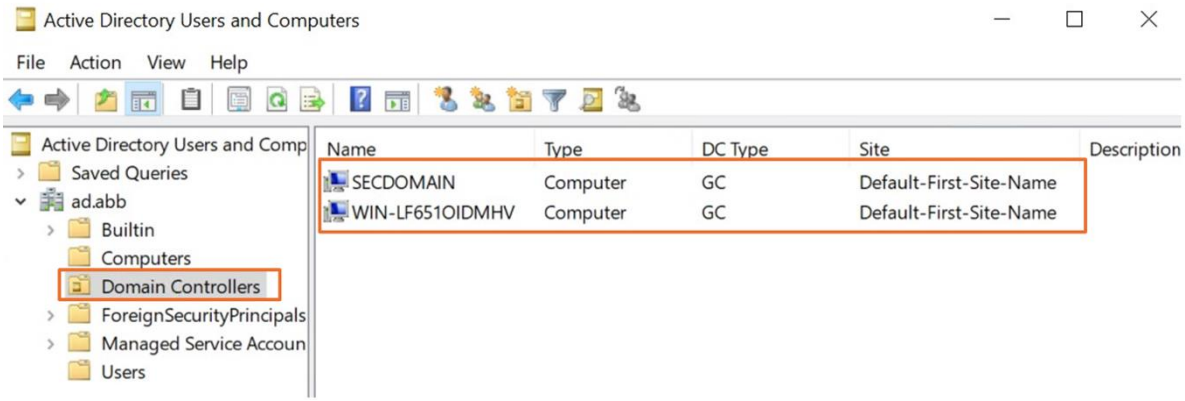
Det grafiske brukergrensesnittet tillater også administrasjon av de virtuelle maskinene, plassere dem i ulike nettverk og VLAN, mulighet for å starte og stoppe dem, samt tilgang til et grafisk konsollvindu for individuell interaksjon med hver maskin, markert med rødt i figur 18.



Figur 18. GUI til VMware, oversikt over virtuelle maskiner

3.3.2 Konfigurasjon av domenet

De fleste av de virtuelle serverne er enheter som ble installert under et felles lokalt domene. På den første virtuelle maskinen, Domain1 (WIN-LF651OIDMHV) som også fungerer som hoveddomenekontroller vist i figur 19, ble *Active Directory Domain Services* (AD DS) satt opp. Serveren er lokalisert på Nettverk-A (VLAN 600) og Nettverk-B (VLAN 700), og ligger på lag 3 i henhold til Purdue-modellen. Rollen og funksjonaliteten til AD DS ble konfigurert gjennom *Add roles*-funksjonen, tidligere illustrert i figur 8. Dette gjør serveren til administrator i domenet, der den oppfyller et av designkriteriene til systemet ved å sikre adgang ved autentisering av brukere. Domenet som ble opprettet på Domain1 er navngitt *ad.abb*.



Figur 19: Domenekontrollerne sin Active Directory Users and Computers (Domain1 Server)

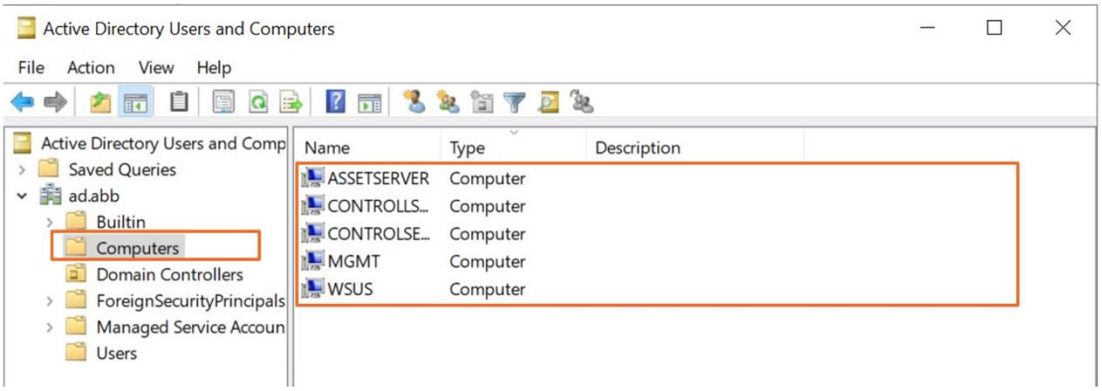
Etter at domenet var satt opp på Domain1-serveren, var neste steg å konfigurere et sekundært domene på Domain2 (SECDOMAIN)-serveren, som skulle fungere som et reservedomene i tilfelle Domain1 skulle slutte å fungere. Denne serveren er også lokalisert på Nettverk-A og -B. Imidlertid møtte vi på utfordringer ved tilkobling; det var da ingen nettverksforbindelse mellom Domain2 og Domain1. Problemet var mangel på en *Domain Name System* (DNS)-tilkobling.

En DNS-tjeneste er kritisk fordi den tillater servere å kunne koble seg til hverandre ved å oversette domenenavn til IP-adresser. Uten denne tjenesten kunne heller ikke de andre serverne etablere forbindelse med domenet. Løsningen ble å installere birollen *DNS-Server* på Domain1. Serveren ville nå fungere som en AD DS med en DNS-Server. Deretter var det mulig for både Domain2-serveren og andre servere i nettverk-A og -B å koble seg til domenet.

Figur 19 illustrerer hvilke servere som er domenekontrollere, og står for håndtering av autentisering ved pålogging, tilgangskontroll, samt autorisere nettverksbrukeres adgang til spesifikke nettverksressurser.

Serverne som ikke var en del av nettverk-A og -B (Management- og WSUS-server) opplevde også problemer med å koble seg til domenet. Til tross for at serverne var korrekt konfigurert med hensyn til fysisk oppkobling, DNS og IP-innstillinger, kunne vi ikke oppnå ping mellom nettverkene. Å finne løsningen på dette problemet var tidkrevende, da det viste seg å være feil i selve oppsettet av ACL på brannmur. I tillegg var det feil med datatrafikk gjennom switchens MAC-adressering. Løsningen på konfigurasjon av switch nevnes i kapittel 3.4.2 og riktig oppsett av ACL nevnes i 3.5.3.1.

For å bekrefte at alle serverne nå var medlemmer i domenet, sjekket vi den administrerende oversikten i AD DS som vist i figur 20. I denne figuren presenteres en komplett liste over alle registrerte servere i domenet, med unntak av de som fungerer som domenet sine kontrollservere. Oversikten gir oss en klar visualisering av domeneinfrastrukturen, og sikrer at alle serverne er korrekt integrert i domenet.



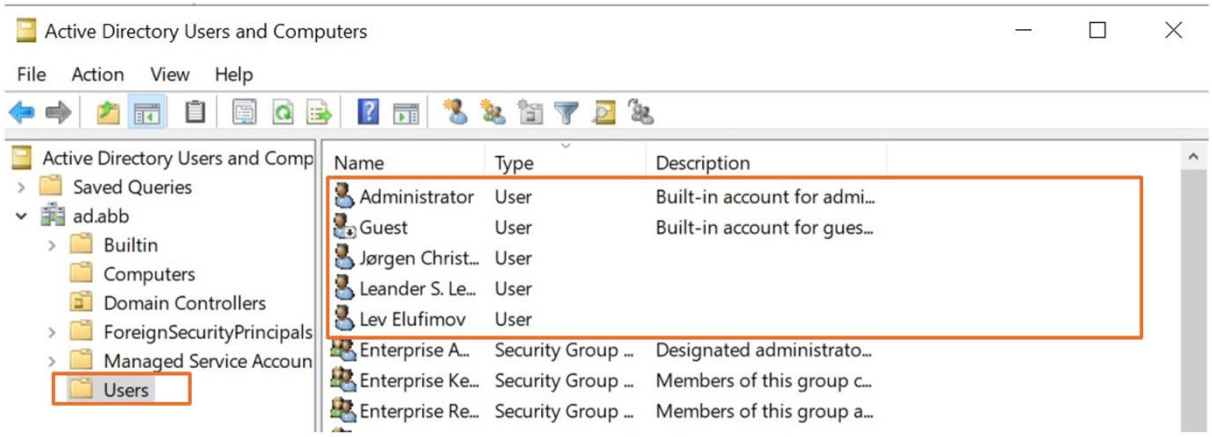
Figur 20: Maskinene i Active Directory Users and Computers (Domain1 Server)

3.3.2.1 Brukere i domenet

Regulering av brukertilganger og definere hvilke rettigheter ulike brukere skal ha for endringer og administrasjon i domenet, kan styres sentralt fra hoveddomenet. Alle tre gruppemedlemmene skulle ha full administratortilgang, og i tillegg var det fra standard en annen generell administrativ brukerkonto (Administrator). Denne kontoen ble beholdt for å tillate at eksterne personer med innloggingsinformasjon kan utføre administrative oppgaver. Eksempler på administrerende oppgaver kan leses i kapittel 2.1.13. Figur 21 viser en oversikt over brukerne i domenet, inkludert en gjestebruker. Gjestebrukeren er satt opp uten tilganger, noe som betyr at den ikke har mulighet til å gjøre endringer eller utføre administrative oppgaver i domenet. Begrensede brukerrettigheter er innført fordi det i noen tilfeller kan være nødvendig for en person å midlertidig samle inn informasjon fra det operasjonelle nettverket. Dette medfører at ulike brukere tildeles spesifikke roller basert på

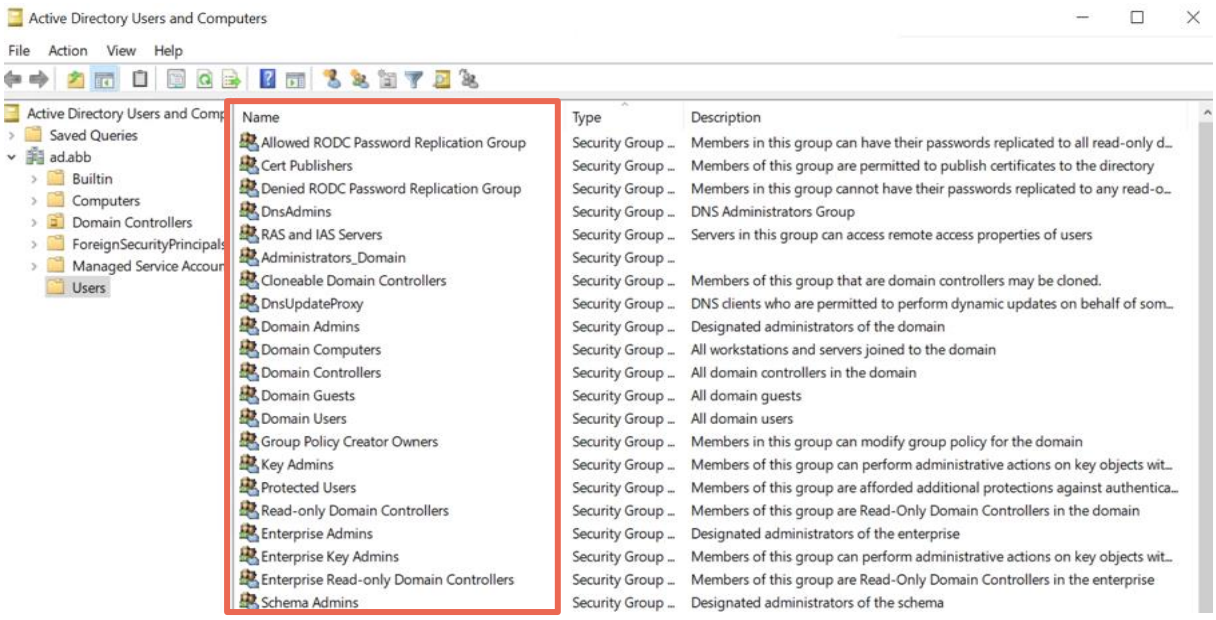
deres behov. En slik bruker vil kun ha mulighet til å utføre de handlingene som er tiltenkt for deres rolle; en sikkerhetsmetode for å kontrollere tilgangen til systemet.

Om det blir nødvending å legge til flere brukere i domenet, har vi muligheten til å bestemme nøyaktig hvilke tilganger hver enkelt bruker skal ha ved å legge de til i ulike *User Groups*. Hver *User group* er satt til å ha forskjellige tilganger, og kan befinne seg i to ulike gruppetyper: *Security group* og *Distribution group*. *Security group* er brukt for å tildele tillatelser til delte ressurser, og *Distributon group* brukes til å opprette e-postdistribusjonslister [16]. I vårt tilfelle brukes det kun *User groups* av typen *Security*, da e-posttjenester ikke skal brukes i vårt nettverk.

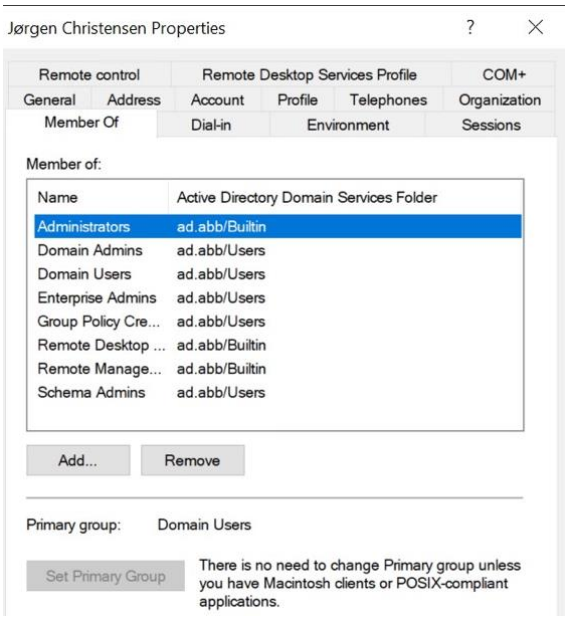


Figur 21: Brukerne i Active Directory Users and Computers (Domain1 Server)

Figur 22 viser ulike grupper som brukere kan bli lagt til i for å få nødvendig tilgang. For eksempel, hvis en ansatt kun skal arbeide med oppdatering av servere, kan vi begrense brukeren ved å tildele kun disse rettighetene. Det å tilpasse tilganger og hvilke *User Groups* de skal legges til i, er illustrert i figur 23. Der kan tilganger legges til eller fjernes for en vilkårlig bruker i domenet. Her demonstreres en bruker vi har gitt full administrasjonstilgang.



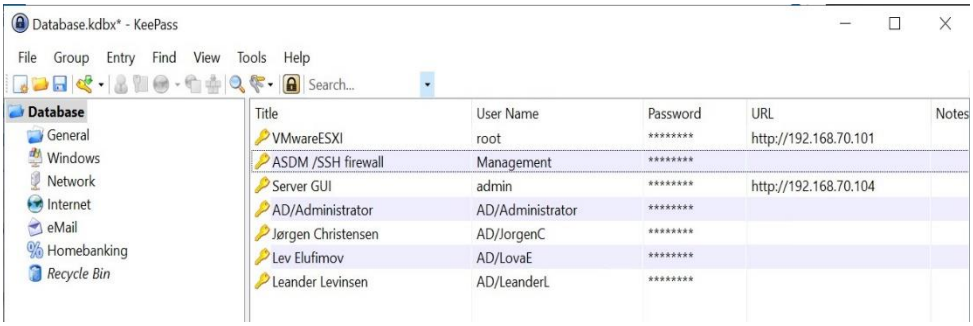
Figur 22: Brukergrupper på domenet



Figur 23: Brukerinnstillinger i domenet

3.3.2.2 Bruk av KeePass

Dette programmet ble tatt i bruk da alle serverne, fjerntilgangene til de fysiske enhetene, og de individuelle brukerne i domenet har autentisering gjennom passordpålogging. For å slippe å huske på, og i tillegg lage alle passordene, måtte vi ta i bruk en passordbehandler. Programmet ble installert på hoveddomenekontrolleren, Domain1. KeePass oppretter en database som lagres i domenet, som gjør at alle serverne som er medlem i domenet har tilgang til å hente ut passordene fra databasen. Figur 24 demonstrerer vår database i KeePass, og all lagret innloggingsinformasjon.



Figur 24: KeePass – opprettet database

3.3.3 Management-server

Management-server ble konfigurert i domenet for å kunne gjøre endringer i nettverkskonfigurasjonen. Denne serveren er plassert i Service-nettverket i VLAN 500, det samme nettverket hvor VMware ESXi og brukergrensesnittene til både switchen og brannmuren også befinner seg, som da tillater serveren å administrere konfigurasjon av VMware ESXi, switch og brannmur. Dette var den første serveren vi satte opp for å forenkle administrasjonen og konfigurasjonen av de andre serverne gjennom ESXi, samt konfigurasjonen av switch og brannmur via deres HTTPs-grensesnitt.

3.3.4 Asset- og Control-server

Asset-server og Control Server 1 og 2 ble lagt til i Nettverk-A og -B, men de er foreløpig ikke tildelt spesifikke driftsroller i det nåværende nettverksoppsettet. Dette skyldes at de nøyaktige arbeidsoppgavene for disse serverne ikke vil bli fastsatt før nettverket tas i bruk, noe som ikke er en del av denne oppgaven. Når nettverket er korrekt oppsatt, er det planlagt at serverne skal konfigureres for bruk i både Nettverk-A og -B. Funksjonen til Asset-server er å fungere som et lagringssted for alle prosjekter, hvor brukere med nødvendige tillatelser kan hente data fra serveren. Hensikten med en Control Server er å kjøre applikasjoner som kommuniserer med enheter som er på de lavere nivåene i Purdue-modellen. Et eksempel på dette kan være en temperatursensor i et kabinett [17].

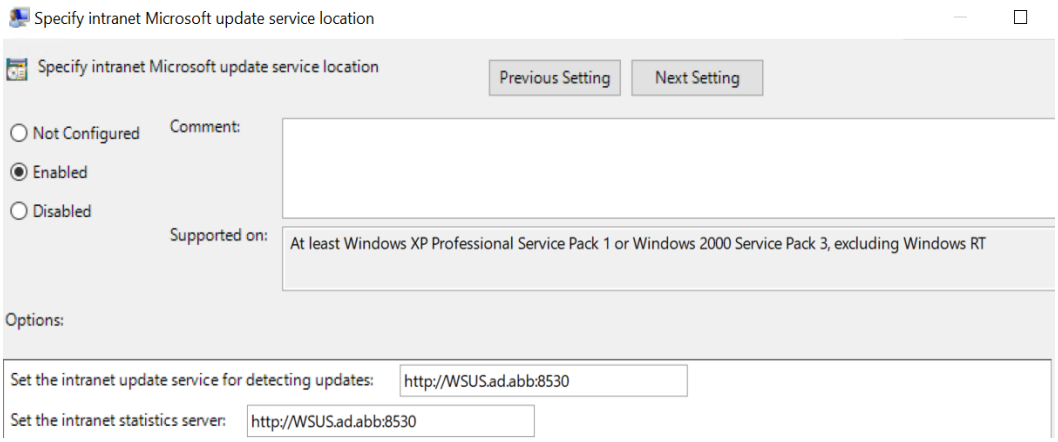
3.3.5 WSUS-server

Windows Server Update Services (WSUS) er ansvarlig for at alle serverne i nettverket holder seg oppdaterte med de nyeste Windows-oppdateringene til enhver tid. For å muliggjøre dette, ble WSUS-serveren installert og plassert i DMZ-nettverket, adskilt fra det interne produksjonsnettverket. Denne lokaliseringen tillater serveren å motta oppdateringer direkte fra Microsoft, eller annen ekstern kilde avhengig av bedriftens praksis. Disse oppdateringene blir deretter distribuert videre til de øvrige serverne i domenet. Dette kan enten gjøres fortløpende, eller i bestemte tidsrom.

For å sette denne prosessen i gang, ble det installert en pakke for en serverrolle kalt WSUS, som inneholder de nødvendige funksjonene for å operere som en oppdateringssentral. I denne pakken finner vi *Framework Features*, *Windows update tools* og *Web Server tools*. Alle er tilleggsfunksjoner som kreves for at serveren kan få tilgang til oppdateringer fra Microsoft og tildele disse videre til de andre serverne som den er ansvarlig for. Oppdateringene administreres gjennom programmet *Update Services*, som er en del av serverrollen til WSUS. Med *Update Services* kan man styre og bestemme hvilke servere i domenet som skal motta oppdateringer.

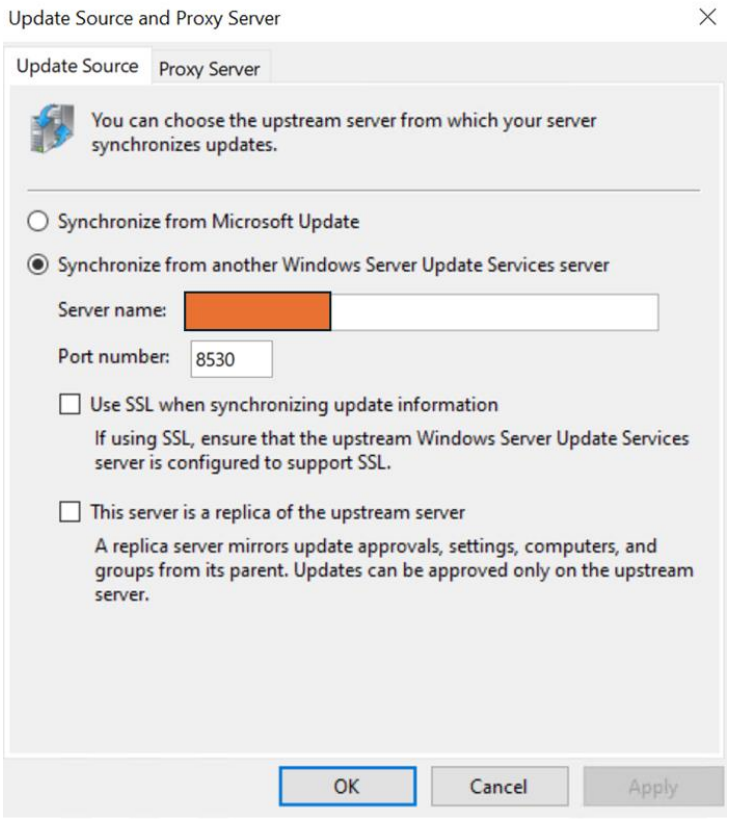
Prosessen viste seg imidlertid å være mer utfordrende enn antatt. Serveren var ikke koblet til Internett under konfigurasjonen, noe som forhindret henting av Windows-oppdateringer. I tillegg oppstod det problemer med å koble de andre serverne i domenet til *Update Services*-programmet. For å etablere en tilkobling mellom WSUS-serveren og de andre serverne i domenet, ble det nødvendig å manuelt konfigurere et *Group Policy Object* (GPO) på domenet. Dette gjorde det mulig å koble oppdateringsuthentingen til WSUS-serveren sin adresse, slik at vi kunne spesifisere hvor de andre serverne i domenet skal hente oppdateringer fra.

Figur 25 illustrerer hvordan oppdateringsuthentingen er konfigurert i domenet. Her blir Windows-oppdateringer oppdaget på port 8530. Dette er standard WSUS Service Port for bruk med HTTP.



Figur 25: Spesifisering av hvor domenet henter oppdateringer

Det ble på sikt klart at vår WSUS-server ikke skal være direkte koblet til Internett, men til ABBs WSUS-server, som igjen er koblet til Microsoft for å hente oppdateringer. Dette ble oppnådd ved å tildele en IP-adresse til ABBs WSUS-server, og tillate gjennom ACL på brannmuren slik at trafikk kan sendes og mottas på port 8530 for den tilordnede IP-adressen. I tillegg måtte vi spesifisere oppdateringskilden i *Update Services*-programmet. Figur 26 viser hvordan man kan spesifisere hvor programmet skal hente oppdateringer fra. Av sikkerhetsmessige årsaker kan ikke den tildelte IP-adressen vises i rapporten.

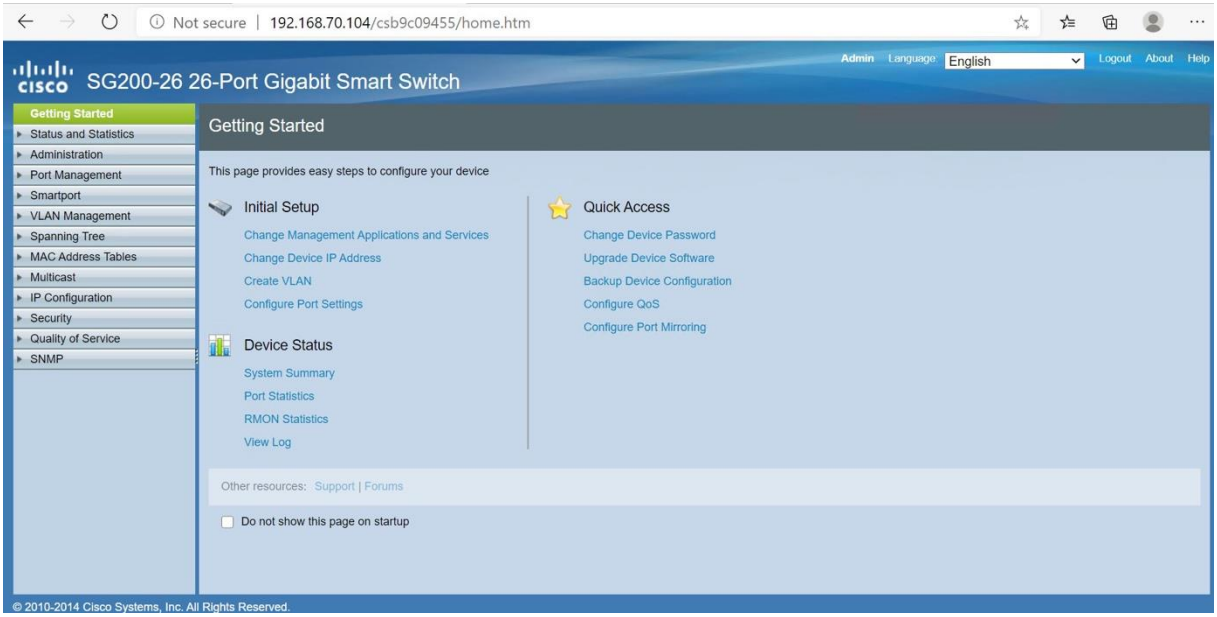


Figur 26: Spesifisering av oppdateringslokasjon på WSUS-Server

3.4 Switch

Opprinnelig fikk vi tildelt en HP2530-switch. Dette viste seg å være en switch med svært begrenset tilgjengelig dokumentasjon, noe som skapte utfordringer med konfigurasjon av SNMPv3, SSH og HTTP. For å løse dette problemet, tok vi saken videre med vår interne veileder i ABB, som tildelte oss en Cisco SG200-switch. Denne switchen var enklere å konfigurere, både fordi vi er tidligere kjent med Cisco-utstyr i *Enterprise*-klassen som har likheter med denne switchen som er i *Small Business*-klassen, men også grunnet Ciscos bedre tilgang på brukerdokumentasjon.

Denne switchen opererer kun med et grafisk grensesnitt via HTTPs i en nettleser, som vist i figur 27. Adressen er ikke teknisk sikret grunnet manglende HTTPs-sertifikat, noe som ikke er uvanlig da nettleseren ikke skiller mellom tilgang via Internett og lokalt. Tilgang er ved brukernavn og passord, og all konfigurasjonen av switchen ble utført her. Det grafiske grensesnittet gjorde det enkelt å ha oversikt over hele konfigurasjonen, i motsetning til å kun ha tilgang til et konsollvindu som er mindre visuelt oversiktlig.



Figur 27: GUI til switch, hjemskjerm

3.4.1 Funksjon

Switchen i nettverket fungerer på lag 2 i OSI-modellen, og bestemmer trafikkering av data basert på serverne sine virtuelle MAC-adresser. Dette gjør den ved å føre en MAC-tabell basert på oppdagede MAC-adresser, og hvilket fysisk grensesnitt de gitte adressene er koblet til. Siden switchen har 26 fysiske grensesnitt, fungerer den derfor som en sentral enhet for å koble sammen enheter i hele nettverket.

I tillegg til å fungere som en type splitter i nettverket, spiller switchen en stor rolle med å segregere hele nettverket inn i mindre og mer håndterbare delnettverk ved bruk av VLAN, både for enkelheten og oversikten, men også for sikkerheten i nettverket. Ved å isolere enheter innenfor mindre deler, er det mulige skadeomfanget i nettverket mye mindre om uvedkommende skulle få tilgang.

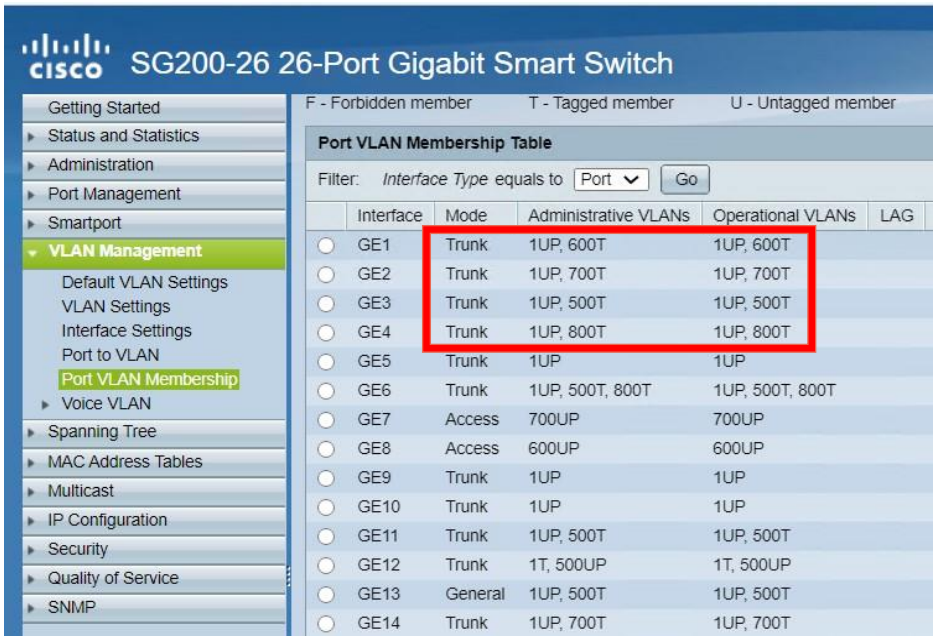
3.4.2 Konfigurasjon

Konfigurasjonsprosessen startet med å tildele switchen en statisk IP-adresse, 192.168.70.104, for administratortilgang, etterfulgt av å sette opp VLAN som beskrevet i tabellen nedenfor.

VLAN	Navn	Adresseområde
500	Management	192.168.70.0/24
600	Nettverk A	172.10.9.0/24
700	Nettverk B	172.11.9.0/24
800	DMZ	10.10.20.0/24

Figur 28: Tabelloversikt VLAN

Deretter ble det konfigurert hvilke fysiske grensesnitt som skulle være Trunk- og Access-ports, samt hvilke VLAN de skulle tilhøre. Figur 29 viser hvordan tildelingen ble konfigurert på port GE1 til port GE4. Vi opplevde her et problem med kommunikasjonen mellom switch, brannmur og server. Årsaken til dette var at noen porter som skulle være Access-porter, i stedet var konfigurert som Trunk-porter. Dette førte til blokkert kommunikasjon mellom enhetene på grunn av VMware ESXi's måte å adressere pakker på i forhold til VLAN. Løsningen viste seg å være mer komplisert enn først forventet, siden switchen ikke tillot oss å endre portenes roller fra Access til Trunk på en enkel måte. Grensesnittet kunne enkelt settes til Access, men ikke like enkelt tilbake til Trunk. Her er man nødt til å endre samtlige innstillinger i ulike menyer i en bestemt sekvens før man kan endre fra Access til Trunk. Etter flere forsøk med å sette grensesnittet sin rolle over til Trunk, fungerte det ved å først fjerne alle VLAN grensesnittet er tilknyttet, så sette grensesnittet sin rolle til Trunk, så tildele VLAN. Dette ville imidlertid vært enklere om switchen hadde hatt konsollvindu i tillegg til det grafiske grensesnittet, da man lett kunne tvunget grensesnittet over på dette med én enkel kommando.



Figur 29: Switch-innstillinger, VLAN-medlemskap per port

Switchen har 26 fysiske porter, men vi trenger ikke flere enn 14. Figur 30 viser under *Port status* at det kun er 8 av de fysiske grensesnittene som er aktive etter endt konfigurasjon, indikert med *Up* i stedet for *Down*. Port GE9 til GE14 ble konfigurert kun for å teste ut tilgang til nettverket med en privat datamaskin, og alle porter unntatt GE1 til GE8 er manuelt deaktivert i etterkant, ettersom ingen flere porter kreves for nettverkets drift. Dette er en sikkerhetsmetode som begrenser antall tilkoblinger til systemet og switchen enn det som er nødvendig, og hindrer dermed uautorisert tilgang som kan forårsake skade.

Figur 30: Oversikt over switchportene og status

3.5 Brannmur

Brannmuren som er tatt i bruk er av typen Cisco ASA 5510, som ble lansert i 2005, og støtte ble avsluttet i 2018. Dette betyr at denne brannmuren har noe begrenset funksjonalitet og sikkerhet sammenlignet med dagens sikkerhetsteknologier og andre brannmurer i faktiske produksjonsmiljø. Grunnet dens alder, er typiske funksjoner som hastighet, programvare, sikkerhetssertifikater for administrasjonstilgang, og detaljerte pakkefiltreringsmetoder utdaterte i forhold til nyere tredjegenerasjonsbrannmurer (NGFW), der disse brannmurene er i stand til å inspisere data på ulike lag i OSI-modellen og har de nødvendige sikkerhetsmekanismene for å møte dagens sikkerhetskrav. Ved bruk av ASA som eneste brannmur, er det mulig for angripere å maskere skadelig trafikk ved å innkapsle dette på et nivå som ASA-brannmuren ikke vil kunne klare å inspisere.

3.5.1 Tre typer administrasjonstilgang

Seriell konsollport: Dette er den enkleste tilgangsmetoden, spesielt nyttig når IP-adressen for SSH- eller HTTPs-tilgang er ukjent. For å oppnå tilgang kobles brannmurens konsollport, markert med blå i figur 31, direkte til en datamaskins USB- eller RS232-port ved hjelp av en Cisco-konsollkabel, eller annen konsollkabel som har lik pin-kontakt for seriell dataoverføring. Datamaskinen bruker en terminalapplikasjon, som *PuTTY* eller *Tera Term*, for å tolke og sende data til og fra brannmuren.

SSH: Er som standard aktivert med IP-adressen 192.168.1.1 på brannmurens egen administrasjonsport, markert med rødt i figur 31. Denne porten brukes ikke for annen nettverkstrafikk enn lokal administrasjonstilgang. De andre fire portene, markert med grønt, er portene for nettverkstrafikk. Siden administrasjonsporten kun brukes for førstegangsoppsett, aktiveres SSH til å være tilgjengelig for alle enheter på Service-nettverket via port 2 i det grønne feltet gjennom denne kommandoen etter at brukernavn, passord og krypteringsnøkler er generert:

Figur 31: ASA 5510 frontpanel

```
ASA-5510-BO24EB-07(config)# ssh 192.168.70.0 255.255.255.0 Service_Network
```

192.168.70.0 er nettverksadressen, og subnettmasken 255.255.255.0 gir alle adresser i Service-nettverket SSH-tilgang. Management-serveren er den eneste enheten i dette nettverket som kan kobles til brannmuren gjennom SSH, VMware ESXi og switchen har ikke SSH-funksjonalitet, dermed er det ikke et sikkerhetsproblem at alle Service-adresser har tilgang.
Vi har spesifisert hele nettverket ettersom vi har brukt våre private PC-er for konfigurasjon.
På grunn av brannmurens utdaterte programvare, nekter Windows' innebygde terminaler å godkjenne utvekslingen av de utdaterte krypteringsnøklene fra brannmuren. Disse nøklene er nødvendige for å etablere en sikker kommunikasjonskanal mellom datamaskinen og brannmuren, ettersom SSH krever innloggingsinformasjon. Dermed brukes *PuTTY* for SSH-tilgang.

Cisco ASDM via HTTPs: *Cisco Adaptive Security Device Manager* (ASDM) er en GUI-basert programvare som kjører via HTTPs for en mer organisert og avansert administrasjon. Oppsett av ASDM var utfordrende på grunn av brannmurens begrensning til TLS 1.0-sertifikater og eldre utgave av Java. Programmet er inkompatibelt med moderne datamaskiner som støtter TLS 1.2 og 1.3, og nyere versjoner av Java nekter å kjøre TLS 1.0-programmer på grunn av sikkerhetsproblemer knyttet

til denne utdaterte TLS-versjonen. Management-server klarer å kjøre ASDM etter installasjon, og det anses ikke noen sikkerhetsproblemer knyttet til bruk av dette programmet. Internettilgang til alle serverne er begrenset, dermed kan ikke uvedkommende utnytte sikkerhetshull i TLS 1.0 og i eldre versjoner av Java for å få tilgang til nettverket.

3.5.2 Funksjon

Brannmuren etablerer og opprettholder kommunikasjonen i nettverket ved å rute trafikken mellom VLAN. Det er ikke behov for en enestående ruter grunnet nettverkets lave omfang og driftskrav. Brannmuren har nok kapasitet til å fungere som både brannmur og ruter her, men i andre tilfeller med større nettverk som krever flere tilkoblinger, kan det være behov for egne rutere eller lag 3-switcher. All trafikk skal i utgangspunktet gå gjennom brannmuren, og dermed vil all data gå gjennom færre ledd dersom man dropper å ha egen ruter som mellomledd mellom switch og brannmur. Dette kan bidra til mindre overhead i form av forsinkelser, men i dette nettverket vil et slikt oppsett ikke ha vesentlig innvirkning på driften og hastigheten.

Siden brannmuren også fungerer som ruter, vil denne enheten også håndtere kontrollering av trafikk via ACL, loggføring av nettverkshendelser via SNMP, og oversetting av eksterne IP-adresser via NAT.

3.5.2.1 ACL

Utenom å rute trafikk, filtrerer brannmuren datatrafikken ved å detektere trafikktype, protokolltype, avsender og mottaker, og gjøre avgjørelser på om datapakkene skal sendes eller kastes basert på konfigurerte regler i ACL. All relevant og nødvendig trafikk skal tillates, som RDP, domene, SNMP og annet for generell kommunikasjon og drift (IP, tidssynkronisering, etc.) mens alt annet skal nektes.

For å gjøre ACL mer lesbart, benytter man *objekt* og *objektgrupper* i form av *service*, og *nettverk*. *Objekter* i nettverk er å navngi IP-adresser til den enheten de tilhører. *Objektgrupper* i nettverk er å gruppere sammen IP-adresser og navngi nettverket, mens *objektgrupper* i service er å gruppere sammen ulike porter/protokoller. Begge disse metodene er for å forenkle konfigurasjon og lesbarhet slik at man kan ha én linje med tillatelser ved gruppering, enn å ha like mange linjer som protokoller man skal tillate mot én IP-adresse eller ett nettverk (illustreres i figur 32 på neste side).

3.5.2.2 SNMP

SNMPv3 brukes for å loggføre alle hendelser i nettverket, og brannmurens rolle er å loggføre når en bruker får eller nektes tilgang for å endre konfigurasjon eller hente data. Dette er for å ha bedre oversikt over nettverket i drift, slik at alle endringer er loggført ved at det er oversiktlig hva som er blitt gjort når, og bruke det til evt. feilsøking dersom det er avvik etter endret konfigurasjon. Brannmuren som er den sentrale enheten i nettverket, og fungerer som ruter, sikrer og kontrollerer også at all SNMP-trafikk sendes og mottas riktig mellom alle enhetene.

Rollefordelingen i SNMP er *agent* og *manager*. Her vil brannmuren, switchen og serverne (ekskludert WSUS) samt feltutstyret være agenter. Disse sender SNMP-meldinger til *manageren*, som i dette tilfellet er WSUS-serveren. På denne serveren vil alle disse meldingene loggføres og kunne sorteres for å ha en enkel oversikt over eventuelle feil i nettverket.

3.5.2.3 NAT

Den eksterne brannmuren er inngangspunktet som brukeren kobler seg til for tilgang til det interne nettverket. Når en bruker med en global ekstern IP-adresse kobler seg til via VPN, blir den eksterne IP-adressen tilordnet en intern IP-adresse innenfor det samme området som den eksterne brannmurens DMZ-nettverk, som er et adresseområde den interne brannmuren kjenner til.

Oppgaven vår er begrenset til å legge til rette for NAT på den interne brannmuren. Den eksterne brannmuren er utenfor vårt ansvarsområde da vi ikke har tillatelse til å endre dens konfigurasjon. Den interne brannmuren tillater koblinger fra den eksterne brannmuren ved å oversette gitte IP-adresser for tilkobling med RDP mot WSUS-server, Management-server og Domain1-server. For det interne nettverket er disse adressene fra den eksterne brannmuren ukjente.

3.5.3 Konfigurasjon

3.5.3.1 ACL

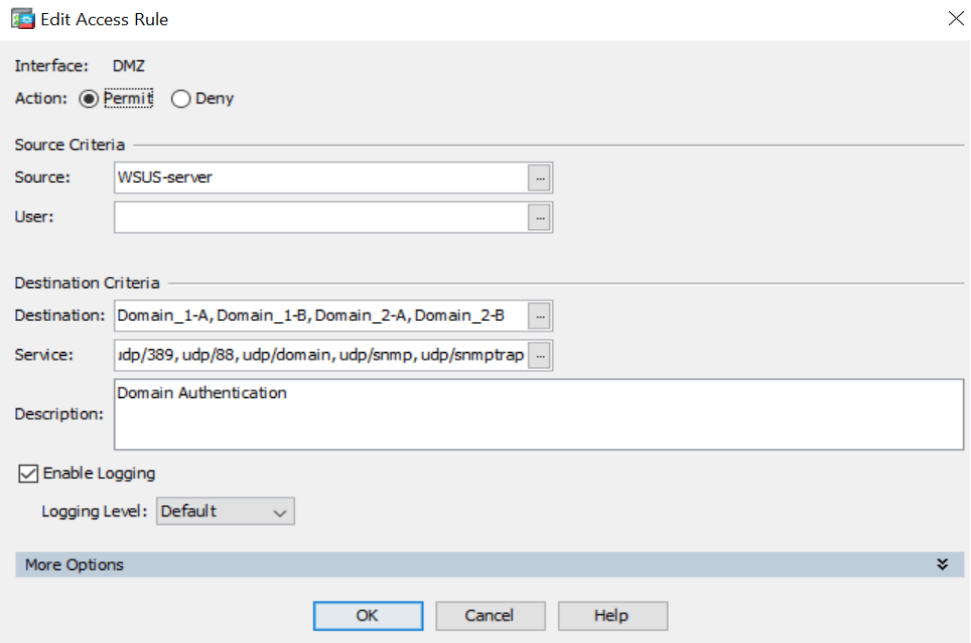
For å planlegge konfigurasjonen av ACL, må man nøye kartlegge hvilken type trafikk som skal tillates og blokkeres for at nettverket skal fungere som tiltenkt. I begynnelsen benyttet vi kommandolinjegrensesnittet fordi vi hadde erfaring med dette tidligere, og ASDM ble ikke satt opp før senere. ACL-konfigurasjon krever grundig planlegging med tanke på rekkefølgen av tillatelser og blokkeringer. Derfor skrev vi først ned alle ACL-reglene i tekstfiler.

Vi fikk tildelt alle tcp- og udp-portnumre for å tillate spesifisert trafikk for at domenet skulle fungere. Til tross for å ha aktivert alle påkrevde porter, var det problemer med at enkelte servere ikke ble lagt til i domenet eller kunne kommunisere med domenet. Det var vanskelig å lokalisere disse problemene grunnet lite samsvar med korrekt konfigurasjon og funksjon. Etter gjennomgang med faglig veileder, fikk vi løst flesteparten av problemene. Enkelte av de mindre vesentlige problemene lot seg ikke løse grunnet manglende tillatelser og utdatert utstyr.

Når ACL var fullstendig utarbeidet, kopierte vi dem fra tekstfil og inn i konsollvinduet for å unngå feil som kan oppstå ved å legge til regler linje for linje og risikere å måtte starte på nytt. Denne tilnærmingen ble valgt fordi denne versjonen av ASA ikke støttet nummererte linjer, som gjør det enklere å håndtere og endre regler i etterkant. Ved å bruke tekstfiler var det enkelt å redigere ACL ved å kopiere og lime inn endringer. Senere da vi fikk tilgang til ASDM, ble konfigurasjonen og oversikten over ACL mye mer brukervennlig og effektiv. I motsetning til å konfigurere linje for linje, som illustrert i figur 32, gir ASDM bedre oversikt og enklere konfigurasjon ved å legge til og fjerne nettverk og protokoller ved å velge gjennom menyer, som vist i figur 33.

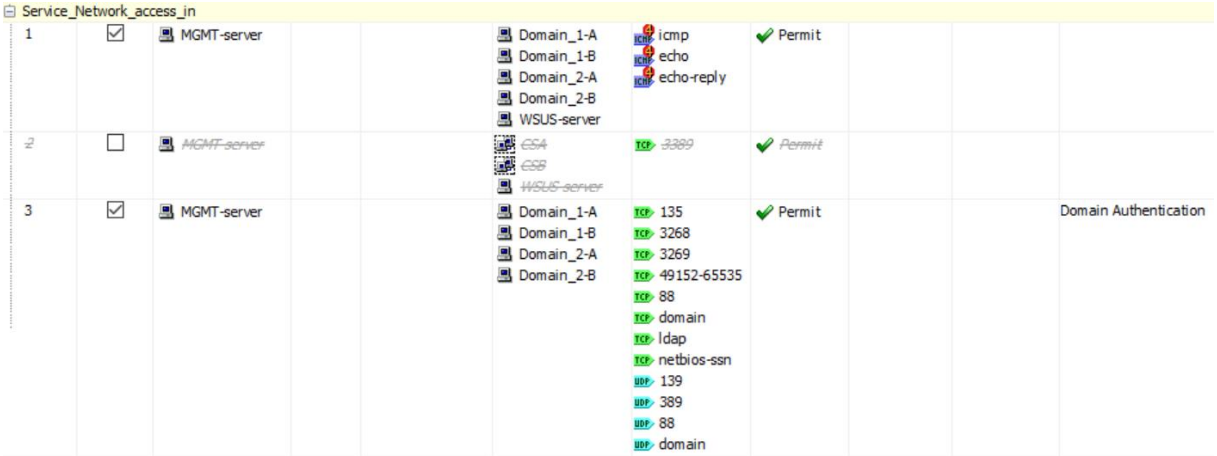
```
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit tcp object MGMT-server object Domain_2-B eq 445
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit tcp object MGMT-server object Domain_2-A eq 445
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit tcp object MGMT-server object Domain_1-B eq 445
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit tcp object MGMT-server object Domain_1-A eq 445
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit tcp object MGMT-server object Domain_1-A range 49152 65535
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit tcp object MGMT-server object Domain_1-B range 49152 65535
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit tcp object MGMT-server object Domain_2-A range 49152 65535
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit tcp object MGMT-server object Domain_2-B range 49152 65535
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit udp object MGMT-server object Domain_1-A range 49152 65535
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit udp object MGMT-server object Domain_1-B range 49152 65535
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit udp object MGMT-server object Domain_2-A range 49152 65535
ASA-5510-BO24EB-07(config)# access-list Service-Access-out extended permit udp object MGMT-server object Domain_2-B range 49152 65535
ASA-5510-BO24EB-07(config)#
ASA-5510-BO24EB-07(config)#
ASA-5510-BO24EB-07(config)# access-group Service-Access-in in interface Service_Network
ASA-5510-BO24EB-07(config)# access-group Service-Access-out out interface Service_Network
```

Figur 32: Utklipp av konfigurasjon av ACL via SSH



Figur 33: Meny for å redigere ACL-regel i DMZ-nettverket

Management- og WSUS-serverne refereres som *object network Management-Server* og *object network WSUS-Server*, mens alle serverne i nettverk-A og -B grupperes sammen som Domene. Alle portene som skal tillates for kommunikasjon mellom alle serverne er også gruppert sammen, mens ICMP (ping) og RDP er gruppert hver for seg. ICMP brukes kun for testing av kommunikasjon og kreves ikke for drift, og kan dermed aktiveres og deaktiveres ved behov. RDP er kun fra bestemte servere mot utvalgte servere. Dette er illustrert i figur 34 der all nødvendig trafikk er aktivert; RDP som har blitt brukt til testing er deaktivert, og ICMP er aktivert i egen gruppering, også for testing.



Figur 34: Service-nettverkets ACL i ASDM

3.5.3.2 SNMP

For at SNMP skal være operativt, må det først aktiveres på brannmuren, og så på alle andre enheter. Deretter må brannmuren vite hvor serveren som skal motta alle meldinger er plassert – i dette tilfellet WSUS-serveren i DMZ-nettverket. Siden vi ikke fikk lisens til å bruke 800xA, har vi kun lagt til rette for at denne programvaren kan installeres.

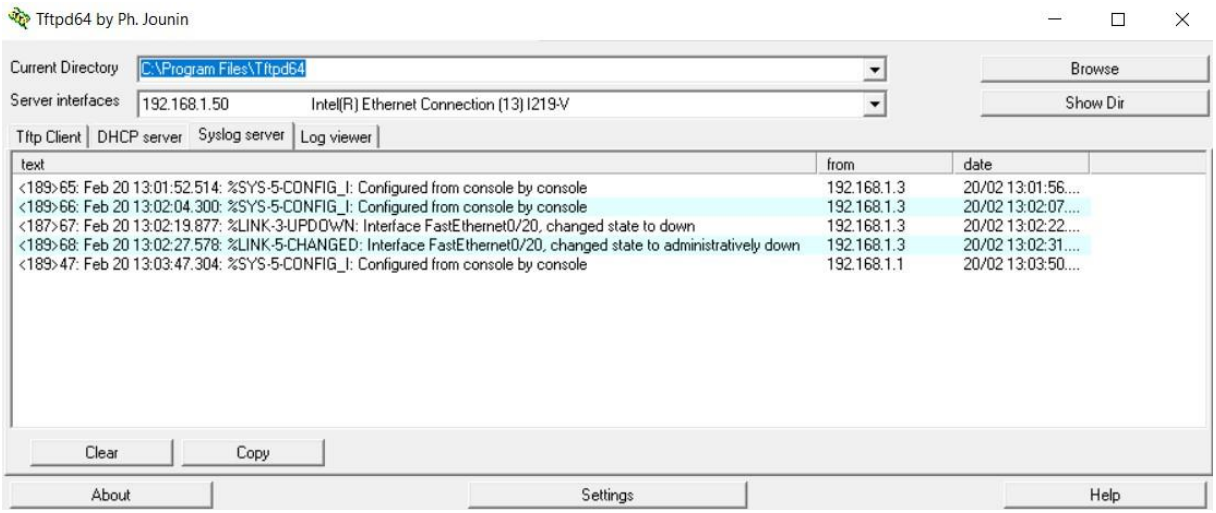
Den oversikten vi kan skaffe i denne oppgaven er begrenset til å overvåke fjerntilkobling, tilkoblinger mellom servere, konfigurasjon av brannmur og switch, og statusmeldinger fra enheter. Ved reell drift, med et tilkoblet prosessanlegg, vil også feltutstyret sende SNMP-meldinger, der mesteparten vil være statusmeldinger. Konfigurasjon av SNMP kan være ganske simpel; illustrert i figur 35:

1. Først aktiveres SNMP
2. En gruppe, *BO24EB-07*, med samme sikkerhetsnivåer lages, her nivået *priv* som tilsvarer autentisering og kryptering.
3. Brukeren *Admin* legges i gruppen *BO24EB-07*, og skal autentiseres ved bruk av *sha*, siden dette er det eneste typen denne brannmuren støtter, og med brukerpassord (*passord1*). For at *Admin* skal få SNMP-tilgang, skal SNMP-meldinger krypteres med et eget AES128-kryptert passord (*passord2*).
4. Serveren er på DMZ-grensesnittet, og det er WSUS-serveren (10.10.20.21) som skal motta SNMPv3-meldingene. Det er her kun *Admin* som skal ha tilgang.
5. Alle typer meldinger, *traps*, skal sendes.

```
ASA-5510-BO24EB-07(config)# snmp-server enable
ASA-5510-BO24EB-07(config)# snmp-server group BO24EB-07 v3 priv
ASA-5510-BO24EB-07(config)# snmp-server user Admin BO24EB-07 auth sha [passord1] priv aes 128 [passord2]
ASA-5510-BO24EB-07(config)# snmp-server host DMZ 10.10.20.21 version 3 Admin
ASA-5510-BO24EB-07(config)# snmp-server enable traps all
```

Figur 35: Konfigurasjon av enkel SNMPv3

Loggføringen av statusmeldinger kan være som demonstrert i figur 36, som viser endring av konfigurasjon gjennom spesifisert protokoll; her via konsoll. Man ser også at det loggføres porter som deaktiveres. Med denne oversikten kan man enkelt kontrollere endringer og feilmeldinger ved å raskt kunne sjekke statusmeldinger. Dette er hentet fra tidligere arbeid med SNMP og syslog, siden vi ikke får tillatelse fra ABB til å installere ikke-godkjent programvare.



Figur 36: Loggføring av konfigurasjon med enkel SNMP-server

3.5.3.3 NAT

For å få tilgang til det interne nettverket fra det eksterne nettverket, måtte enhetene tildeles en ekstern nettverksadresse. IP-adressene ble tildelt av ABB, og er ikke globale adresser, men for vårt nettverk, kategoriseres de som eksterne IP-adresser da de tilhører ABBs DMZ-nettverk. Vi måtte sikre at de eksterne IP-adressene ble oversatt til de korrekte interne IP-adressene via NAT ved å spesifisere hvilke IP- adresser som skulle oversettes. Figur 37 illustrerer hvilke servere som har fått tildelt eksterne IP-adresser. Grunnet ABBs retningslinjer for bedriftssikkerhet, kan ikke de faktiske DMZ-IP-adressene nevnes i rapporten, men IP-adressene 100.10.1.1, 100.10.1.2 og 100.10.1.3 brukes som eksempel.

Server	Intern IP	Ekstern IP
Domain1	172.10.9.1	100.10.1.1
Management	192.168.70.50	100.10.1.2
WSUS	10.10.20.21	100.10.1.3

Figur 37: NAT av intern IP mot ekstern IP (eksempel)

Brannmuren er konfigurert til å oversette de eksterne IP-adressene, da dette er den eneste enheten som har forbindelse med eksterne nettverk via direktekobling mot ekstern brannmur. De interne nettverkene kjenner ikke til andre nettverk enn sine egne, og kan ikke se at tilgang adresseres utenfra, da all kommunikasjon er ved bruk av intern IP-adresse via brannmuren.

3.6 Remote Desktop (Eksternt skrivebord)

3.6.1 Lokal tilgang

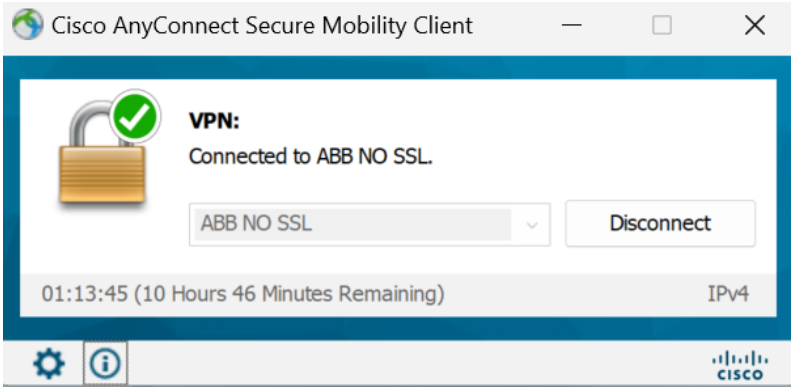
For å få tilgang til alle serverne i nettverket, må man tillate fjerntilkobling til alle serverne fra ett bestemt område – det samme området som brukeren har tilgang til ved tilkobling utenfra. Via Management-server har brukeren tilgang til VMware ESXi, og har lokal tilgang til alle de virtuelle maskinene på den fysiske serveren. Dette er kun tiltenkt for å kunne endre konfigurasjon og feilsøke på maskinvarenivå, og ikke relatert til operasjonell nettverksdrift grunnet mangelfull loggføring.

DMZ-nettverket fungerer som en bro for å få tilgang til andre servere i Nettverk-A, Nettverk-B og Service-nettverket ved å koble til dem eksternt via RDP. Dermed sendes all trafikk gjennom switchen og brannmuren i samsvar med nettverkets design og operasjonelle krav. Tilgang til serverne via VMware ESXi vil ikke kunne loggføres som tiltenkt, og eventuelle sikkerhetskrav vil ikke bli ivaretatt fordi nettverket ikke er klar over den type tilgang som ikke er gjennom nettverksadressering.

3.6.2 Ekstern tilgang

For at brukeren skal få tilgang til OT-nettverket utenfra, må den eksterne brannmuren, administrert av ABB, tillate logiske lokale tilkoblinger for videre adgang gjennom VPN. Den interne brannmuren trenger kun å tillate at koblingen fra den eksterne brannmuren godkjennes inn mot DMZ-nettverket gjennom NAT. Som nevnt i kapittel 3.5.2.3, vil brukerens eksterne IP-adresse oversettes til en lokal IP-adresse i samme område som den eksterne brannmuren sitt DMZ-nettverk, her allokert til IP-adressen 100.10.2.1 (eksempel) som tillater denne brannmuren å opprette en lokal tilkobling mot WSUS-server, Management-server og Domain1-server via RDP og NAT.

VPN-tilkoblingen vår ble konfigurert på en ABB-PC. Figur 38 viser en aktiv tilkobling til ABBs VPN, som er koblet til deres testnettverk.



Figur 38: Aktiv VPN tilkobling gjennom Cisco AnyConnect

Under normal drift, er all tilgang til nettverket eksternt via VPN. Dette er fordi serverne er de eneste enhetene som befinner seg i det interne nettverket. Serverne tillater RDP-tilgang gjennom DMZ-nettverket, hvor DMZ-nettverket igjen tillater tilkoblinger fra den eksterne brannmuren som er i et eksternt nettverk; de interne serverne har ingen kommunikasjon mot eksterne nettverk til tross for at vi er en ekstern bruker. Den eksterne IP-adressen maskeres som en intern IP-adresse.

4 Testing av løsning

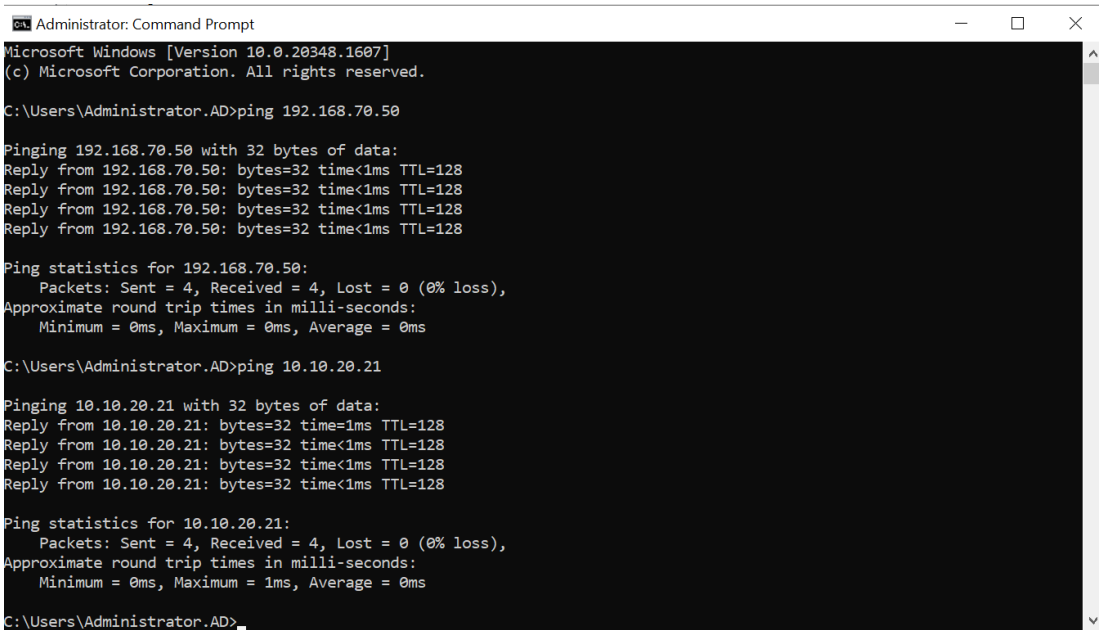
Dette kapittelet presenterer metodene vi har brukt til å teste den implementerte løsningen. Da det ikke er et krav i oppgaven at vi skal installere OT-systemer på serverne, er ikke dette en del av testingen. Denne delen går mer ut på funksjonaliteten og sikkerheten av selve nettverket, at trafikk kommer frem til riktig sted, og overvåkningen ved endt konfigurasjon. Kapittelet er delt opp i to deler: «Testing under konfigurasjonen» og «Testing etter endt konfigurasjon» på grunn av at testing er en stor og viktig del av arbeidet innen nettverksteknologi.

4.1 Testing under konfigurasjon

4.1.1 Ping

Ping er et verktøy som brukes under konfigurasjonsfasen, og er vanlig praksis i både oppsett og feilsøking på grunn av sin enkelhet og effektivitet. Ved å sende ICMP-pakker til enheter i nettverket, kan man fort verifisere tilgjengeligheten av disse, i tillegg til å få oversikt over responstiden og et eventuelt pakketap.

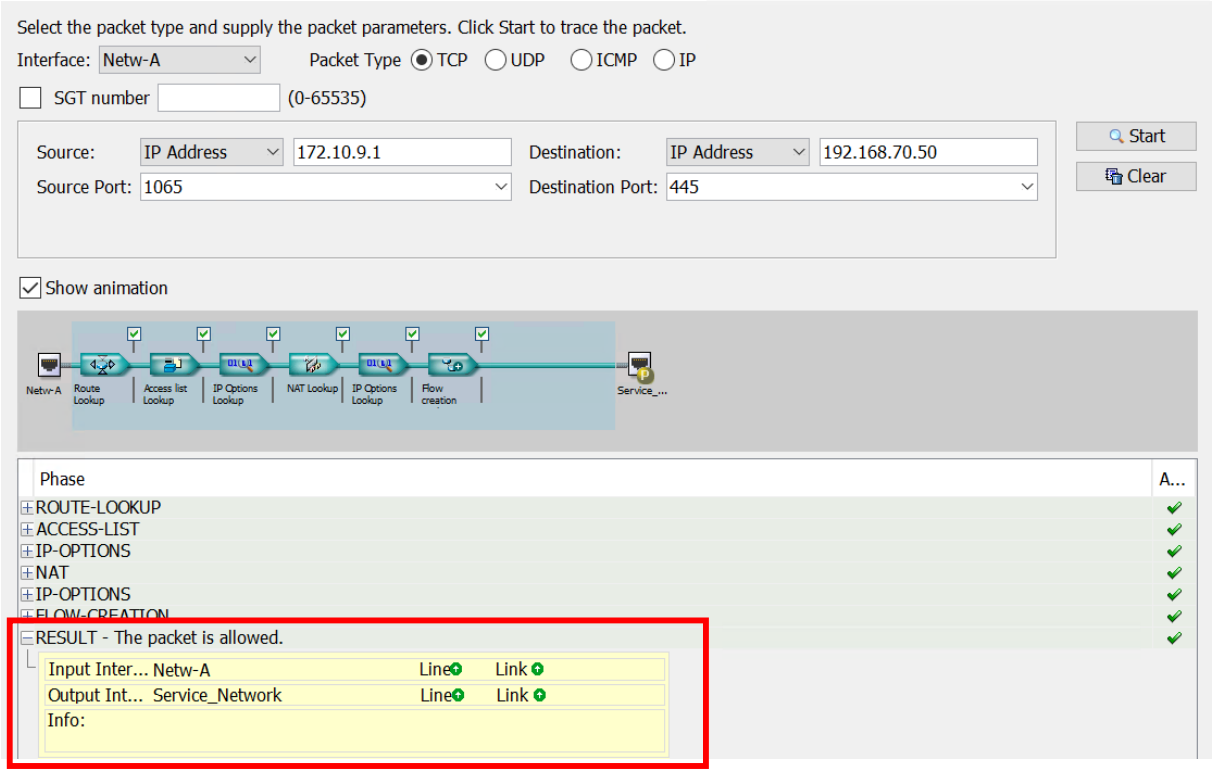
Vi har i konfigurasjonsfasen brukt ping som hovedverktøy for feilsøkingen i nettverket. Grunnen til at vi valgte å bruke dette så mye er både enkelheten og informasjonen det gir oss. Dette verktøyet har gitt oss forståelse for hvor eventuelle koblingsfeil ligger, og bekreftelse på fungerende ruteveier. Figur 39 bekrefter testing av to suksessfulle pingtester, en fra Domain1 (172.10.9.1) til Management-server (192.168.70.50), og en til WSUS-server (10.10.20.21).



Figur 39: Test ved ping fra Domain1 til Management og WSUS

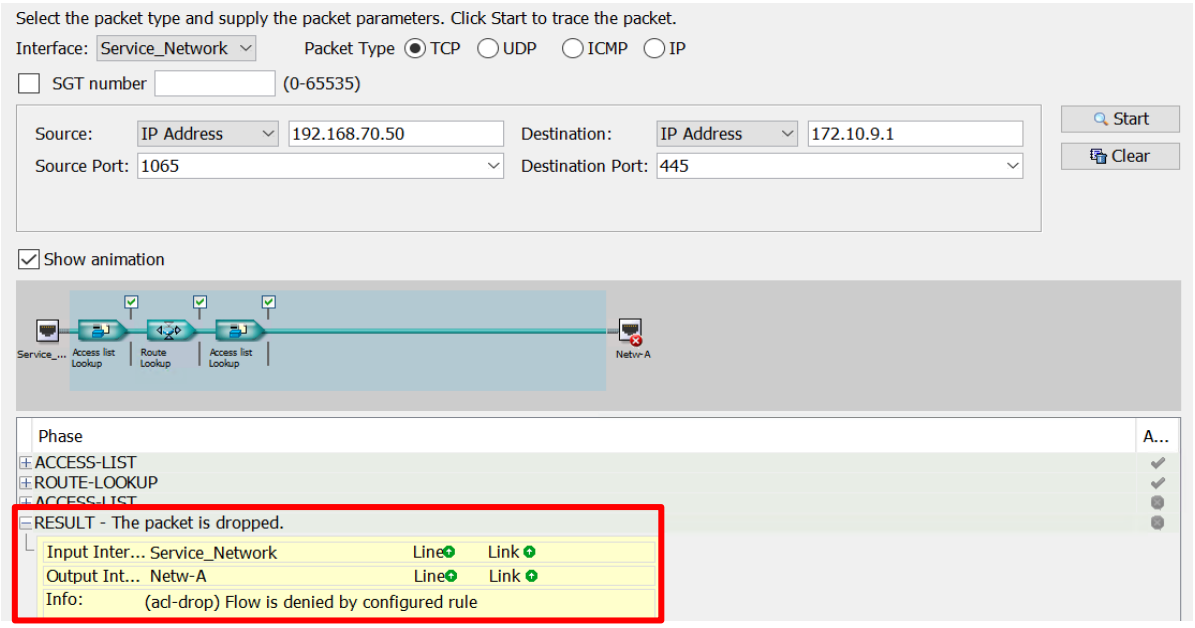
4.1.2 Packet Tracer

Vi har brukt Packet Tracer, som er et verktøy på Cisco-enheter, i testingen av ACL på grunn av funksjonen dette verktøyet har ved å kunne velge portnummer for å simulere sending av datapakker. For eksempel kan man simulere filoverføring ved å sende på port 445 som vist i figur 40, der resultatet av denne testen er at en slik pakke tillates. Her vist i ASDM, men kan også brukes via konsollvindu.



Figur 40: Packet tracer fra Domain1 til MGMT

Det andre eksempelet (figur 41) viser en pakke som blokkeres av ACL fordi Domain1-server skal ikke motta filer fra Management-server. ACL blokkerer pakken basert på konfigurerte regler.

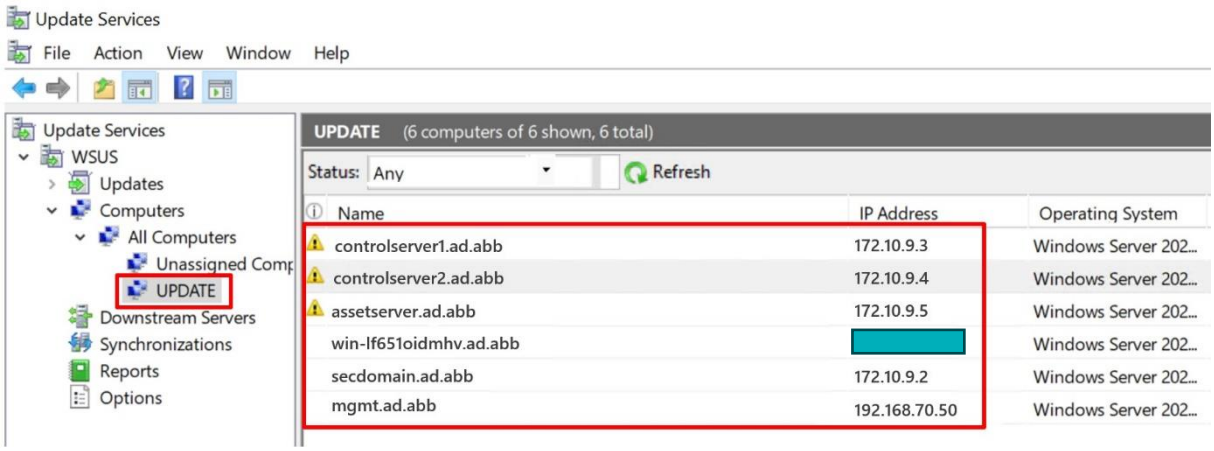


Figur 41: Packet tracer fra MGMT til Domain1

4.2 Testing etter endt konfigurasjon

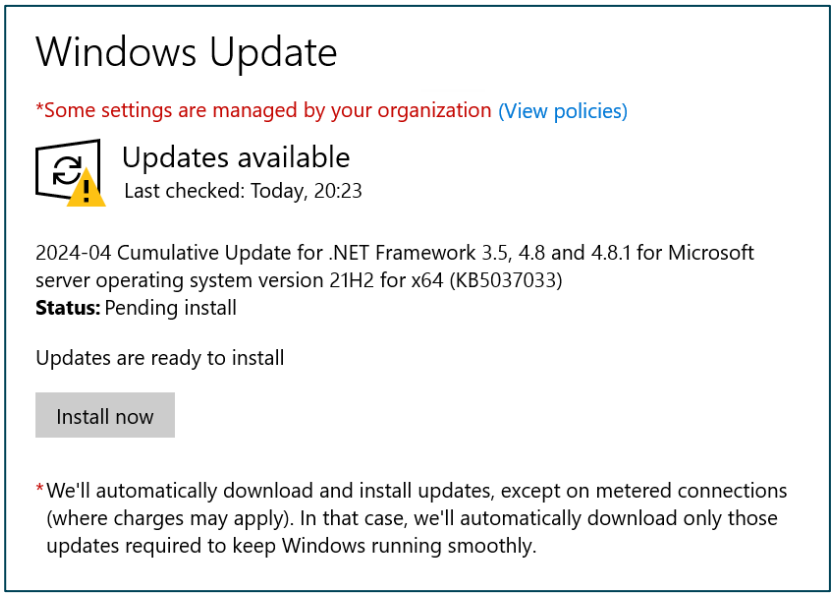
4.2.1 Test av Windows Updates Services

WSUS-server kjører programmet *Update Services.* I figur 42 kan man se en liste over alle servere som er konfigurert til å motta Windows-oppdateringer. Alle tiltenkte servere er til stede i denne listen. Her tester vi også at alle serverne ligger i listen, og om de kan motta oppdateringer fra WSUS-serveren. Om de ikke skulle ligge i listen, mangler det riktig konfigurasjon mellom WSUS-server og de andre serverne. Disse enhetene er plassert i en egen mappe (UPDATE) for å gruppere serverne som skal motta de samme oppdateringene. Hvis noen enheter befinner seg utenfor denne mappen, vet vi at de ikke er del av samme gruppe, eller representerer en ny tilkoblet enhet.



Figur 42: Update Services på WSUS-serveren.

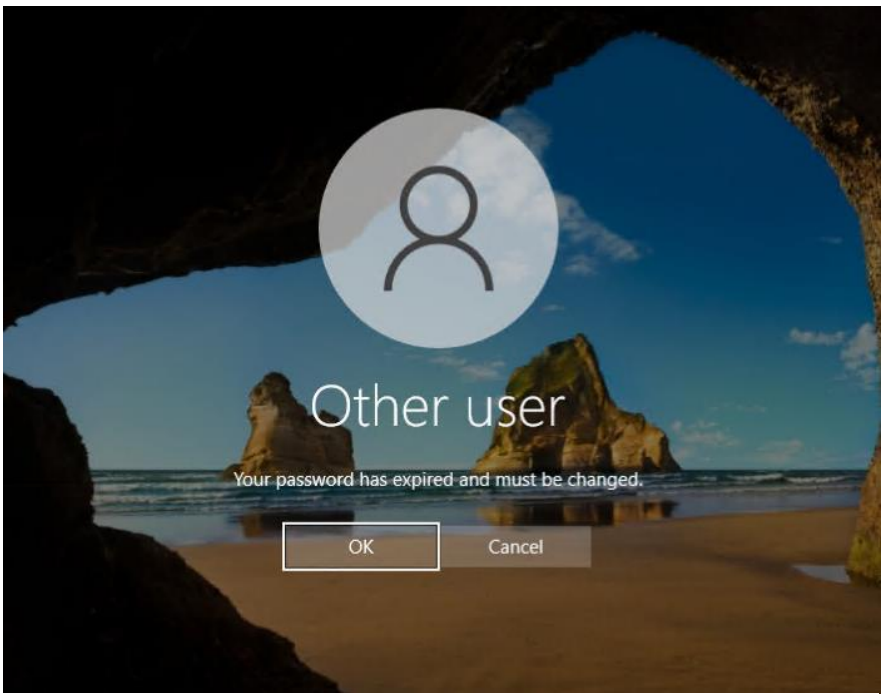
I tillegg må vi sjekke at enhetene på listen mottar oppdateringene fra WSUS-serveren. Vi testet ved å sende en oppdatering fra *Update Services* til alle enhetene i UPDATE-mappen, og sjekket at alle enhetene mottok oppdateringen. Figur 43 viser en mottatt oppdatering på Domain1-server som er klar til å installeres.



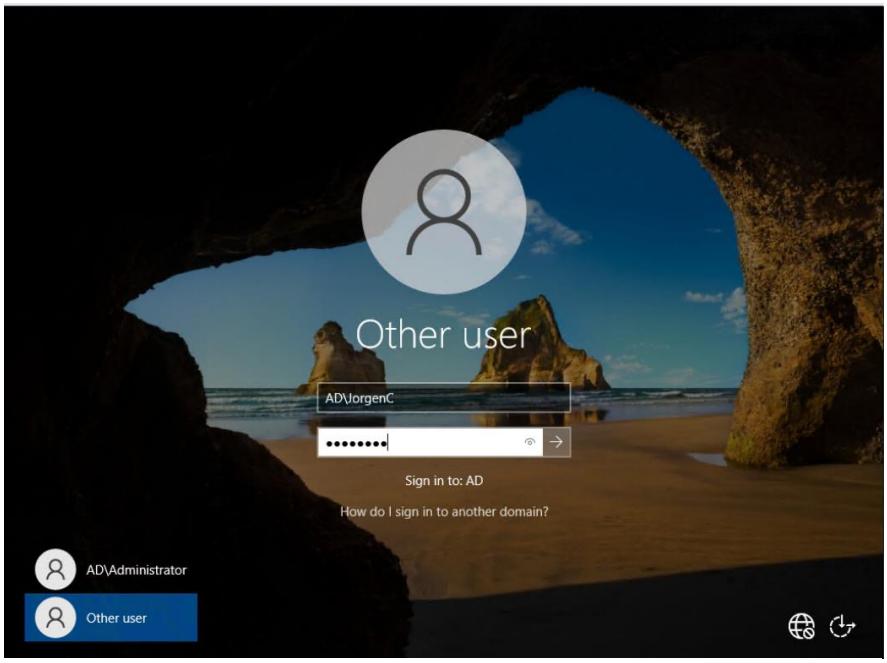
Figur 43: Varsel om tilgjengelig Windows-oppdatering

4.2.2 Test av pålogging for brukere

Vi har testet domenet for å se om det er mulig å logge inn på de ulike serverne med de personlige administratorbrukerne vi har opprettet. Dette fungerer både når hoveddomene-serveren er på, og når den er slått av, noe som indikerer at vår redundante løsning med to domenekontrollere fungerer som planlagt. Figur 44 viser at brukeren "JorgenC" har logget inn i stedet for en standard upersonlig administratorbruker. I tillegg er alle passord i domenet satt til å måtte byttes annenhver uke av sikkerhetsmessige årsaker, som er standardpraksis. Dette betyr at brukeren må endre passord etter to uker for å fullføre innloggingen. Figur 45 viser en test som bekrefter at brukeren får beskjed om at passordet ikke er byttet på to uker og må dermed byttes.



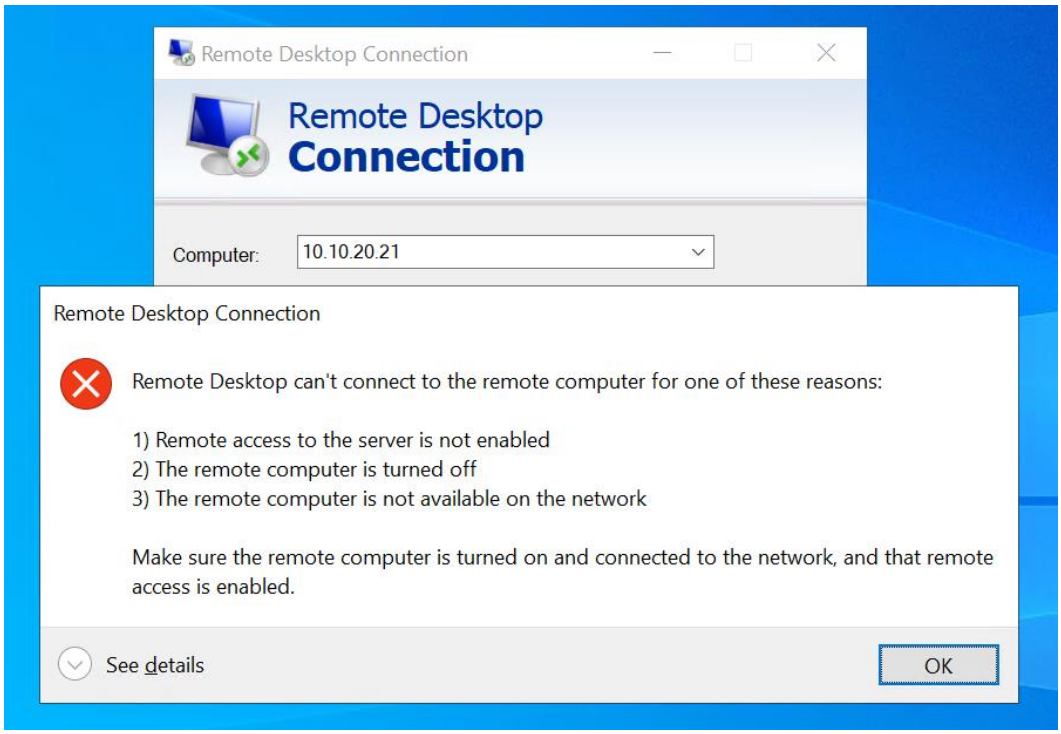
Figur 44: Beskjed om passordbytte for bruker



Figur 45: Pålogging ved egen bruker. her: Jørgen sin bruker

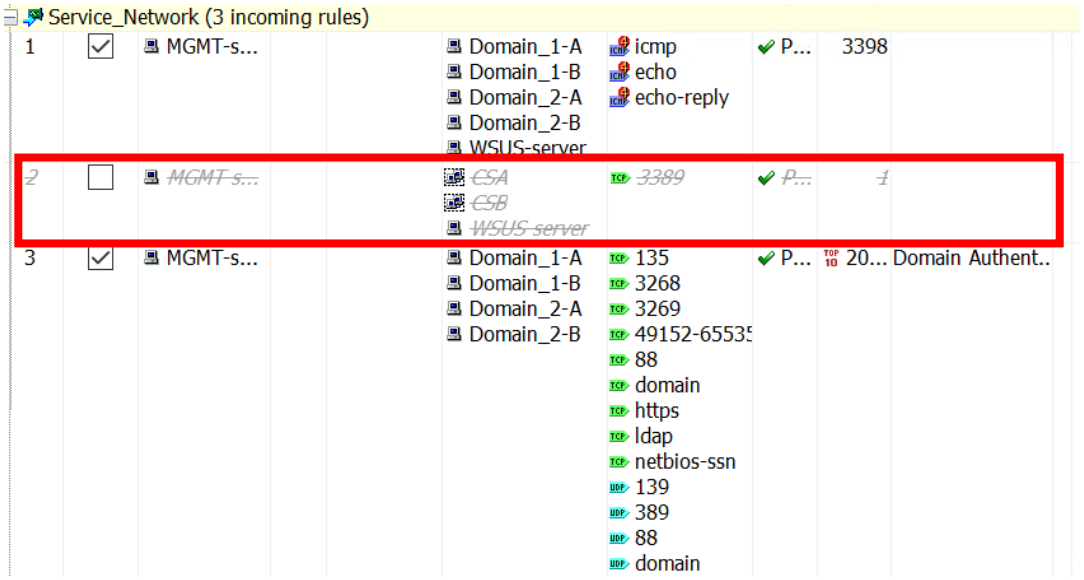
4.2.3 Test av begrenset tilgang med RDP

I nettverket skal det være begrensninger på hvilke servere som har fjerntilgang til andre servere. Figur 46 viser et eksempel på feilmeldingen som dukker opp når man prøver å starte en RDP-tilkobling fra Management-serveren til WSUS-serveren, noe som samsvarer med designet.



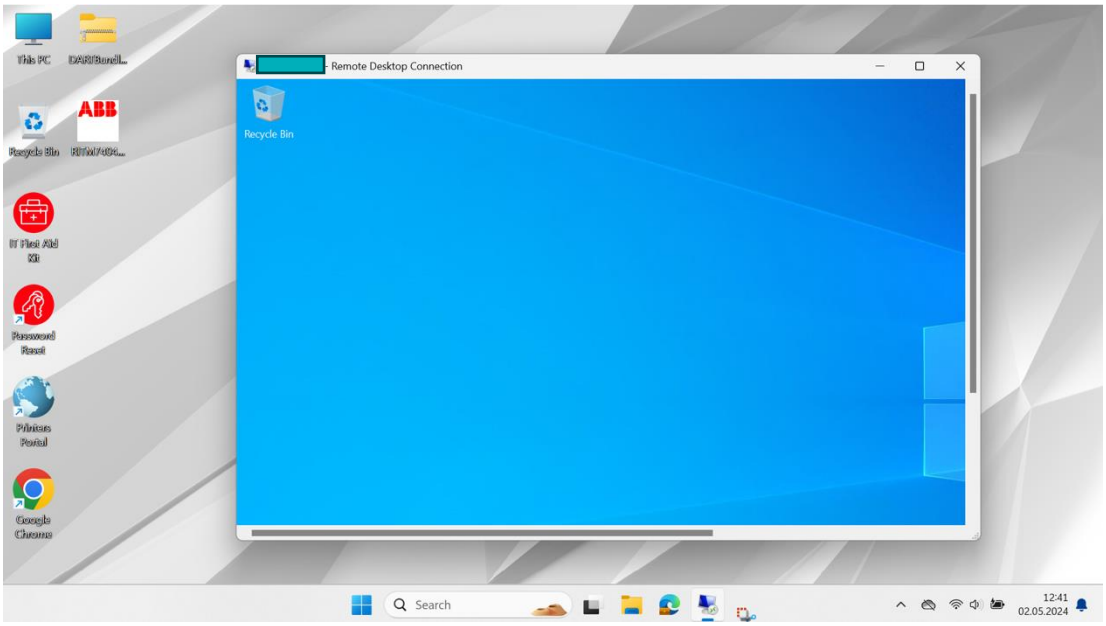
Figur 46: Mislykket forsøk på RDP

Dette har vi utført ved å ikke åpne port 3389 for RDP i ACL mellom de forskjellige nettverkene. I den røde markeringen i figur 47 kan man se at port 3389 er midlertidig stengt mellom Management-server og de andre serverne. Dette kan gjenåpnes av nettverksadministratorer dersom ønskelig eller nødvendig, for eventuell feilsøking eller testing.



Figur 47: ACL for Management-server til Network A, B og WSUS-server

For å kunne jobbe eksternt uten en fysisk tilkobling til serverne, må vi teste om de tildelte eksterne IP-adressene gir oss tilgang til interne enheter via RDP. Management-, WSUS- og Domain1-server har hver fått en ekstern IP-adresse som oversettes ved hjelp av NAT. Ved å være innlogget på ABB-nettverket, eller koble til via VPN, kan vi sjekke om RDP gir oss tilgang. Figur 48 viser en vellykket tilkobling til Domain1 via en ekstern enhet, i dette tilfellet fra en utlånt ABB-PC.



Figur 48: Aktiv RDP-kobling fra en ABB-PC

5 Diskusjon

5.1 Reell bruk av nettverket

Siden dette nettverket ikke er operativt, eller er tenkt til å brukes i faktiske produksjonsmiljø, har vi ikke installert noen kontrollsystemer på lag 2 med styring på lag 3 i henhold til Purdue-modellen. Oppgaven stiller ikke krav til oppsett av programvare for operasjonell drift. Allikevel er nettverket konfigurert for å kunne installere kontrollsystemer ved å endre nettverkets konfigurasjon for å tilfredsstille aktuelle kontrollsystemers krav, slik at nettverket kan testes for reelle brukstilfeller.

Et OT-nettverk blir brukt i industrien for å styre forskjellige prosesser og feltenheter som maskiner og sensorer. Dette kan være alt fra en temperatursensor, et kamera eller en vannturbin. Signalene for disse måledataene vil da først gå gjennom en PLS (*programmerbar logisk styringskontroller*), som igjen vil sende signalet over IP-adresser til serveren. Kommunikasjonen i slike tilfeller vil være gjennom Control-server 1 og -2, hvor informasjonen ville blitt loggført, og det ville også blitt en mulighet for å gjøre endringer på eventuelle innstillinger på feltenhetene. Dette gjøres ofte gjennom applikasjoner for styringssystem som er spesialtilpasset for slik kommunikasjon, for eksempel SCADA.

Domene-serverne står for autentisering og autorisasjon av brukere og enheter i nettverket. Her kan IT-personell velge hvilke tilgangsnivåer enheter og brukere skal ha i nettverket. For eksempel kan man få administratortilgang for å endre alle innstillinger, eller kun lesetilgang for å innhente data.

Asset-server er plassert i nettverket der man kan finne og administrere fysiske ressurser i OT-miljøet som nettverket er satt opp i. Dette fungerer som et inventar over alle enheter i nettverket, og man kan få opp informasjon som for eksempel IP-adresser, plassering, tag-nummer, og når det sist var kommunikasjon mellom utstyr og server.

Management-server i vårt tilfelle er kun en server hvor vi har tilgang til å endre på nettverkskonfigurasjonen (fysisk server, switch og brannmur), og er plassert i Service-nettverket. Arbeid som skjer på denne serveren vil ikke være en del av operasjonell drift, men administreres heller av IT-personell når det blir rapportert feil i nettverket, eller for å endre på innstillinger for systemets drift på nettverksnivået; ikke relatert til de operasjonelle systemene.

WSUS-server står for å innhente oppdateringer for Windows Server 2022. Den vil derimot ikke installere det på serverne med én gang, men gjøre det ved et gitt tidspunkt på dagen. Her kan det være bra praksis å for eksempel sette av installeringstid til den tiden på døgnet det er minst trafikk, eller aktivere reservenettverk og -servere for å oppdatere uten å måtte stoppe driften.

5.2 Systemsikkerhet og videreutvikling

Siden systemet i denne oppgaven ikke er en prototype, men en implementasjon av et eksisterende produkt, vil graden av sikkerhet være i henhold til virksomhetens generelle retningslinjer, da systemet ikke er satt til å utføre bestemte oppgaver. Dette betyr at systemet per nå er som et skall for å verte kontrollsystemer, dermed er systemet kun sikret med tanke på adgang utenfra og inn mot serverne fordi ingen kontrollsystemer er i drift eller installert. Nettverket vil allikevel fungere som en sikkerhetsbarriere mellom usikrede eksterne nettverk og sårbare kontrollsystemer.

All tilgang og funksjonalitet er regulert gjennom grunnleggende retningslinjer som forsøker å oppfylle definerte sikkerhetskrav så godt som mulig, selv om det er visse begrensninger grunnet utstyrets alder og manglende oppdateringer. Dette inkluderer bruken av brannmur som ikke lengre mottar sikkerhetsoppdateringer eller annen form for støtte siden 2018, noe som innebærer at sikkerhetshull avdekket etter 2018 vil kunne være en sårbarhet for systemet, fordi det ikke kan fikses. Dette er en kjent problematikk, men allikevel er det metoder for sikker bruk av utdatert maskinvare.

Sikker bruk av utdatert brannmur er plassering av enheten slik at sikkerheten til andre systemer ikke vil bli svekket. Dette kan være å isolere brannmuren bak andre oppdaterte brannmurer som kan filtrere trafikk som den utdaterte brannmuren ikke kan. Siden nettverket i denne oppgaven skal ha begrenset funksjonalitet, samsvarer dette med brannmurens begrensede funksjoner sammenlignet med moderne standarder for høyere nivåer av sikkerhet og funksjoner. Dermed er det unødvendig å oppgradere enhetene til nyere modeller som fortsatt får produsentstøtte for å møte dagens strengere sikkerhetskrav, gitt systemers økende kompleksitet. Vår brannmur er en del av et lukket internt nettverk med én kobling mot en ekstern brannmur som kan ivareta sikkerheten til det interne nettverket, ved at denne er mellomleddet mot usikret Internett.

6 Konklusjon

Gruppen har gjennomført oppgaven i henhold til utarbeidet oppgavebeskrivelse som tilfredsstiller forventningene til ABB. Nettverket tillater fjerntilkobling mot alle krevde punkter via NAT, og tillater ønsket trafikk samtidig som all uønsket trafikk nektes. Domenet gir nødvendig administrering av enheter og brukere, i tillegg har det en fungerende reserveløsning som tar over ved eventuell svikt der brukere kan fremdeles logge inn gjennom domenet. Loggføring er satt opp for installasjon av programvare, men grunnet manglende tillatelse for å bruke ABBs programvare for SNMP, har ikke dette vært testet i henhold til beskrivelsen – ved installasjon vil dette fungere som tiltenkt.

Nettverket har noe begrenset funksjonalitet sammenlignet med det ABB utvikler for faktiske produksjonsmiljø. Sikkerheten til systemet er det eneste i oppgaven som totalt tilfredsstiller ABBs krav og samsvarer med deres praksis, og som er oppgavens sentrale tema.
I den opprinnelige oppgaveteksten ble det nevnt at oppgaven skulle løses i henhold til IEC 62443 og designes ut ifra Purdue-modellen. Dette har hatt sine begrensninger grunnet at ABB ikke kunne utlevere dokumentasjon om IEC 62443-standarden, som har ført til at vi ikke har kunnet tolket dens beskrivelser direkte. Standarden og Purdue-modellen definerer segmentering av nettverk i ulike soner for ulike behov og bruk, samt tilfredstillelse av ulike sikkerhetskrav i et sammensatt system. Nettverket vi har konfigurert tilfredsstiller krav om sikker kommunikasjon mot utsiden, og mellom de ulike sonene i nettverket i henhold til IEC 62443 og Purdue-modellen.

Arbeidsflyten har vært jevn og med gode marginer. Ved utarbeidelse av forprosjektet var det uklart hva oppgaven faktisk definerte, samt beregne tidsbruken på hver milepæl. Alle frister har blitt overholdt, og det har ikke vært problemer å gjennomføre arbeidet tidsnok. Dette har skyldtes et godt samarbeid i gruppen, og en god kommunikasjonskanal med våre veiledere, Adis Hodzic ved HVL og Nikhil Raj Gupta ved ABB.

Resultatet av prosjektet er nødvendigvis ikke det tekniske utfallet, da dette ikke vil bli tatt i bruk av ABB, men heller læringsprosessen og ferdighetsutviklingen, særlig innen konfigurasjon, nettverkssikkerhet og nettverkplanlegging. Oppgaven har hatt en høy vanskelighetsgrad knyttet til konfigurasjon og forståelse av server-delen, ettersom dette fagområdet ikke inngår i studiet og gruppemedlemmene hadde begrenset forkunnskap. Det har også vært utfordringer grunnet begrensninger til utstyr med utdatert programvare og manglende støtte for moderne sikkerhetsmekanismer. Dette har ført til at nettverket måtte designes rundt det utstyret vi arbeider med faktisk kan støtte, siden vi ikke kunne bruke de nyeste og mest sikre løsninger, har vi heller gjort alternative konfigurasjoner for å tilfredsstille oppgave- og sikkerhetskravene.

Gjennom arbeidet har vi fått en bedre forståelse for, og lært oss hvordan nettverk kan designes etter spesifikke krav for IT- og OT-systemer – en verdifull innsikt i en nettverksingeniørs arbeidshverdag.

Referanser

[1] «Om oss - Let's write the future together,» ABB, 2024. [Internett]. Available: https://new.abb.com/no/om-oss. [Funnet 7 Mai 2024].

[2] «Cyber security,» ABB, [Internett]. Available: https://global.abb/group/en/technology/cyber-security. [Funnet 15 Januar 2024].

[3] «ISA/IEC 62443 Series of Standards,» ISA, [Internett]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Funnet 1 Februar 2024].

[4] B. Edgeworth, R. H. D. Garza Rios og J. Gooley, i *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide*, Cisco Press, 2020, p. 4.

[5] T. Bårdgård, «TCP, UDP og porter,» 12 Mai 2022. [Internett]. Available: https://ndla.no/subject:26f1cd12-4242-486d-be22-75c3750a52a2/topic:6e8a2eaf-4983-4d42-a9b0-911b5921b44a/resource:1aeca2b5-6233-401f-bd3f-7a6127afe9d5. [Funnet 8 April 2024].

[6] T. H. N. Eirik Rossen, «Store Norske Leksikon,» 31 Mai 2023. [Internett]. Available: https://snl.no/domene_-_IT. [Funnet 7 Mai 2024].

[7] Microsoft, «Active Directory Domain Services Overview,» 17 August 2022. [Internett]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview. [Funnet 8 April 2024].

[8] Microsoft, «Microsoft Learn,» 31 August 2016. [Internett]. Available: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11). [Funnet 16 April 2024].

[9] A. K. Linda Rosencrance, «TechTarge,» September 2019. [Internett]. Available: https://www.techtarget.com/searchwindowsserver/definition/Group-Policy-Object. [Funnet 16 April 2024].

[10] A. S. Gillis, «WMware ESXi,» TechTarget, [Internett]. Available: https://www.techtarget.com/searchvmware/definition/VMware-ESXi. [Funnet 26 April 2024].

[11] «What is the difference between server roles and features?,» 4 August 2023. [Internett]. Available: https://eitca.org/cybersecurity/eitc-is-wsa-windows-server-administration/working-with-windows-server/launching-windows-server/examination-review-launching-windows-server/what-is-the-difference-between-server-roles-and-features/. [Funnet 4 April 2024].

[12] H. Liang, S. Xu og L. Chen, «Understanding the Remote Desktop Protocol (RDP),» Learn Microsoft, 26 Desember 2023. [Internett]. Available: https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol. [Funnet 26 April 2024].

[13] P. O'brien, «Integrated System Cybersecurity: Understanding and Applying IEC 62443-3-3,» exida, 12 Juli 2019. [Internett]. Available: https://www.youtube.com/watch?v=IjlMR0EaXJk&t=1617s. [Funnet 15 Mars 2024].

[14] W. Stallings, i *Network Security Essentials, Applications and Standards, Sixth edition*, Pearson, 2017, pp. 187-207.

[15] «KeePass Password Safe,» [Internett]. Available: https://keepass.info. [Funnet 15 April 2024].

[16] T. P. S. J. K. T. Daniel Simpson, «Microsoft learn,» 8 September 2023. [Internett]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups. [Funnet 2024 April 29].

[17] National Institute of Standards and Technology, «Control Server,» [Internett]. Available: https://csrc.nist.gov/glossary/term/control_server. [Funnet 16 April 2024].

[18] «Bringing IT & OT Security Together, Part 2: BAS and the Purdue Model, Security Boulevard,» 2023. [Internett]. Available: https://securityboulevard.com/2023/06/bringing-it-ot-security-together-part-2-bas-and-the-purdue-model/. [Funnet 15 Januar 2024].

[19] H. Haugerud, «operativsystem,» 22 August 2020. [Internett]. Available: https://snl.no/operativsystem. [Funnet 11 April 2024].

[20] B. Posey, «Techtarget,» April 2019. [Internett]. Available: https://www.techtarget.com/searchwindowsserver/definition/Group-Policy. [Funnet 16 April 2024].

[21] «ABB ICS Cyber Security Reference Architecture,» ABB, 2024. [Internett]. Available: https://new.abb.com/process-automation/process-automation-service/advanced-digital-services/cyber-security/abb-cyber-security-reference-architecture. [Funnet 22 April 2024].

Forkortelser og ordforklaringer

ACL	Access Control List (Adgangskontrollister)
AD	Active Directory
AD DS	Active Directory Domain Services
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
DMZ	Demilitarized Zone
DNS	Domain Name System
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
HTTPs	Hyper Text Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IP	Internet Protocol
IT	Information technology (Informasjonsteknologi)
LAN	Local Area Network (lokalnettverk)
MAC	Medium access control
NAT	Network Address Translation
NGFW	Next-Generation FireWall
OS	Operativsystem
OSI-modell	Open Systems Interconnection Basic Reference Model
OT	Operational Technology (industriell nettverksteknologi)
PLS	Programmerbar Logisk Styring
RDP	Remote Desktop Protocol
SCADA	Supervisory Control And Data Acquisition
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network (virtuelt lokalnettverk)
VPN	Virtual Private Network
WSUS	Windows Server Update Services