

Prosjekt:

# Nytt Strålesenter Telemark

Tittel:

## D17.2 Arkitektur – Nettverk og Sikkerhet i Helse Sør-Øst

01	Utgitt for konkurranse	17.01.25	Lise H. Habbestad
Rev.	Beskrivelse	Rev. Dato	Utarbeidet av
Kontraktor/leverandørs logo:		Bygg nr:	Etasje nr.:
		Systemgr.:	Antall sider:
		<b>Side 1 av 37</b>	
Prosjekt:	Opphav:	Fag:	Dok.type:
<b>STRÅLE</b>	<b>0000</b>	<b>N</b>	<b>KO</b>
Løpenr:		Rev.nr.:	Utgiv.kode
<b>0008</b>		<b>01</b>	<b>G</b>

# Revisjonstabell


Rev.	Kapittel	Endring	Navn
01	-	Utgitt for konkurranse	Lise H. Habbestad

Prosjekt:

## Fellesaktiviteter Nye sykehus

Tittel:

# Arkitektur – Nettverk og Sikkerhet i Helse Sør-Øst

04	Lagt til mer tekst, løst opp kommentarer	22.03.24	TORRE T			
03	Lagt til mer tekst, ryddet i struktur	15.12.23	TERIVE			
02	Tidlig utkast for gjennomlesing	12.10.23	TORRE T			
01	Nytt dokument opprettet	04.04.23	TORRE T			
Rev.	Beskrivelse	Rev. Dato	Utarbeidet	Kontroll	Godkjent	
Kontraktor/leverandørs logo:		Bygg nr:	Etasje nr.:	Systemgr.:	Antall sider:	
					Side 3 av 37	
Prosjekt:	Kontrakt nr:	Fag:	Dok.type:	Løpenr:	Rev.nr.:	Status:
HSØ	8250	F	RA	0002	04	G

Kontaktpersoner:

Rolle	Navn	Epost	Telefon
Prosjektleder	Liz Tandberg	<a href="mailto:liztan@sykehuspartner.no">liztan@sykehuspartner.no</a>	+47 46 93 05 63
Teknisk design	Torbjørn Retterås	<a href="mailto:torret@sykehuspartner.no">torret@sykehuspartner.no</a>	+47 90 97 57 04
Teknisk design	Terje Kval Iversen	<a href="mailto:terive@sykehuspartner.no">terive@sykehuspartner.no</a>	+47 90 61 22 20
Tjenesteansvarlig	Rune Bjørn Amundsen	<a href="mailto:ruamun@sykehuspartner.no">ruamun@sykehuspartner.no</a>	+47 95 77 86 91

## Ordliste

<i><b>Forkortelse</b></i>	<i><b>Forklaring</b></i>
AD	Active Directory
ADC	Application Delivery Controller (Applikasjonslastdeling)
AP	Access Point
API	Application programming interface
BGP	Border Gateway Protocol
CERT	Computer Emergency Response Team
CsC	Carrier Supporting Carrier
DNAC	Cisco Digital Network Architecture Center
EAP	Enrollment for Application Platform
EAP-TLS	EAP Transport Layer Security
HSØ	Helse Sør Øst
HTTPS	Hypertext Transfer Protocol Secure
IaC	Infrastructure as Code
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IPSec	Internet Protocol Security
IPv4	Internet Protocol versjon 4
IPv6	Internet Protocol versjon 6
LAN	Local Area Network
LDS	Lokalt Datasenter-nettverk
LTSN	Lokalt Tilpasset Server-nettverk
MAB	Mac Authentication Bypass
MAC	Media Access Control
MTU	Medisinsk Teknisk Utstyr
OOB	Out-Of-Band
PoE	Power over Ethernet
QoS	Quality of Service
RHF	Regionalt Helse Foretak
RIP	Routing Information Protocol versjon
RR	Route Reflector
RSSI	Received Signal Strength Indication
SDA	Software Defined Access
SDN	Software Defined Networking
SDS1	Sentralt DataSenter 1
SDS3	Sentralt DataSenter 3
SGT	Scalable/Security Group Tag
SHKR	Sentralt Hoved Kommunikasjon Rom
SSID	Service Set Identifier
TLS	Transport Layer Security
VCS	Version Control System
VLAN	Virtual Local Area Network
VN	Virtual Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless LAN
WLC	Wireless LAN controller

WPA  
WTP

Wi-Fi Protected Access  
Wan Tilknytnings Punkt

## Innholdsfortegnelse

Ordliste .....	5
Innholdsfortegnelse .....	7
Sammendrag .....	8
1 Innledning .....	9
1.1 Bakgrunn .....	9
1.2 Hensikt .....	9
1.3 Målgruppe .....	9
1.4 Avgrensninger .....	9
1.5 Avvikshåndtering .....	10
2 Overordnet beskrivelse av nettverk i Helse Sør-Øst .....	10
3 Arkitekturprinsipper for nettverk i Helse Sør-Øst .....	11
4 Overordnede sentralfunksjoner i Helse Sør-Øst .....	11
4.1 Organisering av nettverkssoner .....	11
4.2 Integrasjoner med hybride- og offentlige skytjenester .....	12
4.3 Orkestrering og automatisering .....	12
4.4 Overvåkning og nettverksdrift .....	13
5 Ekstern aksess WAN .....	14
5.1 Stamnett fra Norsk Helsenett .....	15
5.2 Virtualiserte transportnettverk .....	15
5.3 Designmønstre for Transportsoner .....	15
5.4 Tilknytningspunkt for WAN (WTP) .....	16
5.5 Regional ekstern aksess .....	16
6 Eksterne nettverk .....	16
6.1 Publisering av tjenester - DMZ .....	17
7 HF-LAN og lokalt datasenter .....	17
7.1 Klassifisering av lokasjoner .....	17
7.2 Lokasjoner .....	18
7.3 Seperasjon mellom helseforetakene .....	22
7.4 Felles kontrollsystemer for Helseforetakets lokalnett (HF-HUB) .....	24
7.5 Brannmur på lokasjonene .....	24
7.6 Policybasert tilgangskontroll .....	24
7.7 Komponenttyper .....	25
7.8 Lokal Datasenterfunksjon .....	27
7.9 Tilgang til nettverksinfrastruktur via Out-Of-Band (OOB) .....	28
8 Trådløst nettverk .....	29
8.1 Generelt .....	29
8.2 Struktur .....	29
8.3 Aksesspunkter .....	29
8.4 WLAN Kontrollere .....	30
8.5 Dekning .....	30
8.6 Klient-VLAN for trådløse klienter .....	31
8.7 WLAN SSID .....	31
8.8 Sporing og lokalisering .....	31
8.9 Sikkerhet .....	32
9 Innendørs Mobildekning 4G/5G .....	32
10 Wifi gjestenett .....	34
11 Nettverksadministrasjon, overvåkning og logging .....	34

11.1	Nettverksadministrasjon .....	34
11.2	Overvåking og logging.....	35
11.3	Sykehuspartner CERT .....	35
	Referanser .....	37

## Sammendrag

Dette dokumentet gir en overordnet beskrivelse av det moderniserte nettverksdesignet for Helse Sør-Øst (HSØ). Moderniseringen av nettverket er forutsetning for en rekke initiativer i Helse Sør-Østs regionale utviklingsplan mot 2040 for å kunne tilrettelegge for mobilitet og nye arbeidsflater, digital hjemmeoppfølging, bygging av sykehus og nye medisin- og byggetekniske løsninger på en sikker og stabil måte. Hensikten med dokumentet er å etablere en felles beskrivelse av nettverksplattformen for å støtte regionens drift, faglige strategier og produktstrategier.

Målgruppen inkluderer byggherrer, prosjektledere, arkitekter og entreprenører. Dokumentet har visse avgrensninger, blant annet unntak for beskrivelse av sentrale datasentre.

Nettverket skal støtte digitaliseringen av helsesektoren, være en regional infrastruktur basert på prinsippet om "Zero Trust," og inkludere verktøy for effektiv drift og forvaltning. Programvaredrevet nettverksplattform (Software Defined Networking) velges for automatisering, rask utrulling av tjenester, bedre innsikt og sikkerhet.

Arkitekturprinsipper inkluderer digitaliseringstilrettelegging, regional infrastruktur, "Zero Trust," effektiv drift, og økt leveransekraft. Transportsoner organiseres basert på sikkerhetspolicyen, og integrasjon med hybride og offentlige skytjenester realiseres gjennom Norsk Helsenett.

Orkestrering og automatisering, inkludert infrastruktur som kode, er gjennomført for effektiv drift. Overvåking og drift bruker maskinlæringssystemer, og ekstern aksess sikrer interoperabilitet mellom HSØs lokasjoner.

Stamnett fra Norsk Helsenett og virtualiserte transportnettverk kobler alle lokasjoner, og designmønstre for transportsoner følges. Regional ekstern aksess sikrer kontroll og perimetersikring. DMZ brukes for publisering av tjenester mot eksterne nettverk.

Nettverket er modulært, og ulike designmønstre brukes for forskjellige lokasjonsklasser (A++, A+, A, B, C og D). Sentrale elementer inkluderer NHN Stamnett/SD-WAN, Fusion for virtualisering, HF-HUB for sentraliserte managementsystemer, Software Defined Access (SDA Fabric), lokasjonsbrannmur, lokalt datasenter (LDS), og nettverk for lokalt tilpassede servertjenester (LTSN).

Lokasjoner er klassifisert basert på kritikalitet, skalering, lokal overlevelse og autonomi. Designet omfatter "Zero Trust"-prinsippet, og datasentre er knyttet sammen gjennom NHN



Stamnett. LDS gir lokal autonomi og robusthet. Lokasjonsspesifikke soner og brannmurer sikrer isolasjon mellom helseforetakene.

Policybasert tilgangskontroll brukes for å autentisere enheter som kobles til nettverket, og IEEE 802.1x og sertifikatbasert autentisering brukes. LDS kan være enten Lokalt tilpasset Server Nettverk (LTSN) eller Lokalt Datasenter Nettverk (LDN).

Felles kontrollsystemer (HF-HUB) administreres sentralt, men hvert helseforetak har sitt eget SDA Fabric domene og kontrollsystem. Lokasjonene følger en felles regional sikkerhetspolicy. Det er etablert brannmurer for isolasjon mellom helseforetak, og lokasjoner med lokal datasenterfunksjon har mulighet for applikasjonslastdeling (ADC) for best mulig ressursutnyttelse og feiltoleranse.

## **1 Innledning**

### **1.1 Bakgrunn**

Dette dokumentet beskriver overordnet design for Helse Sør-Østs (HSØ) moderniserte nettverksplattform. Modernisert nettverksplattform er en leveranse i program for standardisering og modernisering av IKT-infrastrukturen i HSØ, besluttet av RHFet i styresak 048-2018.

Dokumentet skal benyttes som arkitekturprinsipp for nettverksinfrastruktur i nybygg, eller ombygging/ rehabilitering av eksisterende lokasjoner i Helse Sør-Øst.

### **1.2 Hensikt**

Formålet med dokumentet er å etablere en omforent beskrivelse av nettverksplattformen som skal etableres og forvaltes. Dokumentet skal gjenspeile nettverksinfrastrukturen som til enhver tid breddes og videreutvikles. Dokumentet skal også understøtte den til enhver tid gjeldende drift, fag- og produktstrategi for datakommunikasjon i Helse Sør-Øst.

En omforent beskrivelse vil bidra til at nettverksplattformen etableres som en enhetlig regional løsning som understøtter helseforetakenes behov.

### **1.3 Målgruppe**

Målgruppe: Byggherre, Prosjektledere, Arkitekter og Entreprenører.

### **1.4 Avgrensninger**

Dokumentet beskriver ikke arkitektur og oppbygging av de sentrale datasentrene (SDSx), som er felles for alle helseforetakene i foretaksgruppen.

## 1.5 Avvikshåndtering

Dersom det besluttet å omgå noen av kravene i dette dokumentet, skal dette avvikshåndteres i henhold til gjeldende prosedyre avtalt mellom Byggherre og SPHF. Som minimum skal dette registreres som en sak i dokument- og saksregistersystemet. Helseforetaket skal også være mottaker av avviksmeldingen.

## 2 Overordnet beskrivelse av nettverk i Helse Sør-Øst

Sykehuspartner HF (SPHF) har behov for å øke sin leveransekraft og endringsevne, samtidig som hele nettverksinfrastrukturen må rigges for en sterk vekst av tilkoblede enheter og styrkede krav til sikring. HSØ vil fremover se at et stadig større antall sensorer, nye typer arbeidsflater og avanserte medisinske og byggtekniske systemer (MTU og BTU) tilkobles nettverket. Nettverket er en av grunnsteinene for å kunne tilrettelegge for denne veksten av komponenter. Mer enn 250.000 interne enheter er i dag knyttet til nettverket i regionen. I underkant av 30% av disse regnes som administrerte PCer. Dette gjelder både innenfor og utenfor sykehusområdene. Mye av veksten forventes i antall trådløse enheter. Ansatte, pasienter og samarbeids-partnere forventer fleksible og mobile løsninger med høy tilgjengelighet og kvalitet.

En standardisert og modernisert infrastruktur vil bedre sikkerheten knyttet til regionens IKT-systemer og medisinsk teknologisk utstyr, samt legge til rette for den teknologiske utviklingen som er avgjørende for å understøtte digitalisering, helhetlige pasientforløp og pasientens helsetjeneste.

### 3 Arkitekturprinsipper for nettverk i Helse Sør-Øst

Nettverksplattformen bygges etter følgende overordnede arkitekturprinsipper:

- Nettverk skal tilrettelegge for digitalisering av helsesektoren i regionen
- Nettverket skal bygges som én regional infrastruktur
- Nettverket skal være basert på prinsippet om <<Zero trust>>
- Nettverksplattformen skal inkludere verktøy for effektiv og dokumenterbar drift og forvaltning av nettverk i regionen
- Økt leveransekraft samt effektiv drift og forvaltning legges til grunn for design og implementering av nettverket

Infrastrukturen skal inneha kapabiliteter for orkestrering og automasjon av funksjoner i nettverket. Sykehuspartner har valgt å ta i bruk programvaredrevet nettverksplattform (Software Defined Networking) for å understøtte dette. Gevinstene ved å ta i bruk en programvaredrevet plattform er blant annet:

- Automatisering av repeterende arbeidsprosesser reduserer muligheter for feil, forenkler drift og administrasjon av nettverket
- Raskere utrulling av nye tjenester og funksjoner i nettverket
- Bedre innsikt og kontroll med proaktiv analyse av trafikk, kapasitet og trender i nettverket
- Økt sikkerhet ved å benytte mekanismer for bedre tilgangskontroll og segmentering i nettverket

Det skal utarbeides et høy- og lavnivå (HLD og LLD) design for helseforetaket og lokasjonene som skal ta imot nettverksplattformen. Dette dokumentet vil være et overbygg og gi generell beskrivelse av hvilke elementer nettverksplattformen kommer med.

Nettverket skal knyttes til helseforetakenes sikkerhetsarkitektur og bygges med fokus på implementasjon av gode sikkerhetskontroller og av nettverkinfrastrukturen i sin helhet. Nettverket er bygget på prinsippene i CIS versjon 8 og Helse Sør-Østs prinsipper for personvern og sikkerhet.

## 4 Overordnede sentralfunksjoner i Helse Sør-Øst

### 4.1 Organisering av nettverkssoner

Nettverket følger føringene for lokal segmentering gitt i [NO-43 Sikkerhetspolicy for Regional Sonemodell v.1.1.](#)

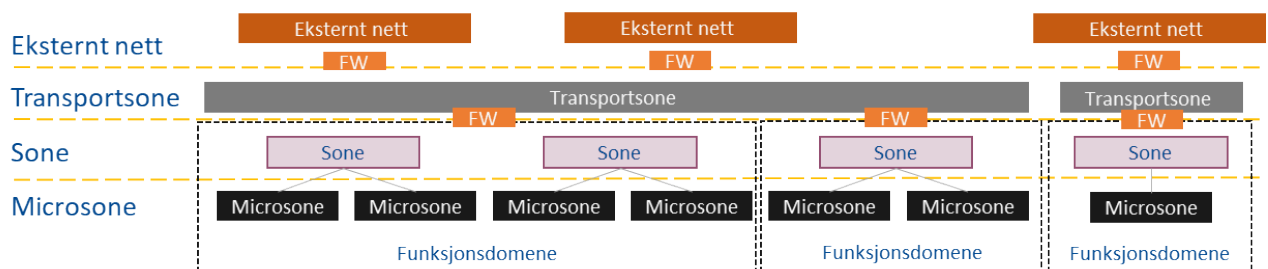
Separering av endepunkter innenfor soner og mikrosoner baserer seg på behovet for separasjon mellom hvert enkelt endepunkt. Det er blitt etablert sikkerhetsmekanismer som skiller mikrosoner innenfor en sone fra hverandre.

Soner vil grupperes i funksjonsdomener. Definisjonen på et funksjonsdomene er ifølge NO-43: «Funksjonsdomene: En logisk avgrenset del av felles plattform som er opprettet for en spesifikk tenant eller funksjon. I Sykehuspartner skilles det mellom "Regionalt funksjonsdomene" for funksjon eller

*tjenester med felles dataansvar, og "HF-spesifikt funksjonsdomene" for spesifikt juridisk foretak med separat dataansvar.»*

Det er etablert transportsoner for å binde sammen funksjonsdomener på forskjellige lokasjoner. Alle soner innenfor ett funksjonsdomene er tilknyttet den samme transportsonen. Det foreligger sikkerhetsmekanismer som skal sikre skille mellom andre transportsoner og funksjonssoner som ikke er knyttet til hverandre.

Transportsoner kan tilkobles eksterne nettverk som internett eller helsenett, men da skal sikkerhetsmekanismene skille transportsone fra eksternt nettverk.



Figur 1: Funksjonsdomener, soner og transportsoner

## 4.2 Integrasjoner med hybride- og offentlige skytjenester

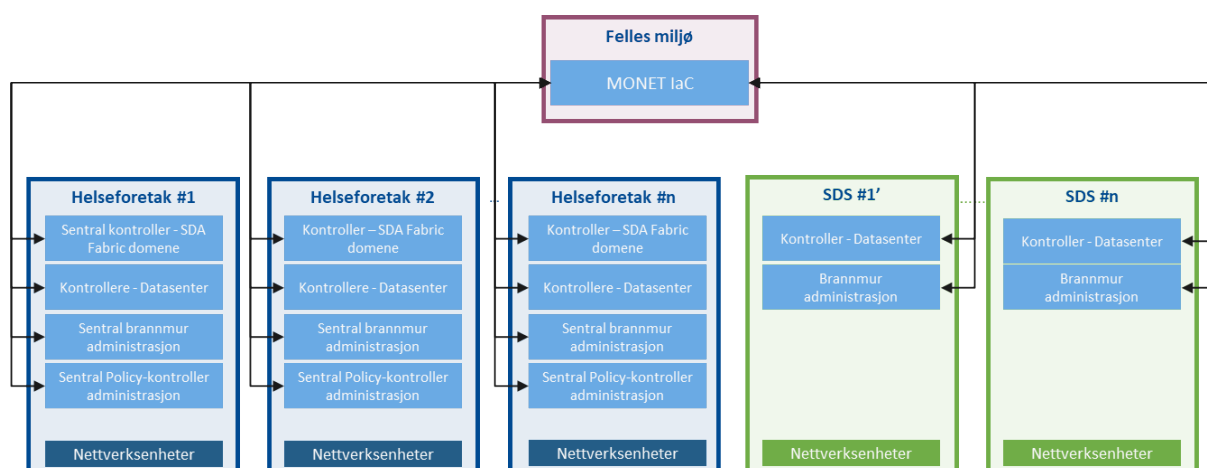
For offentlige skytjenester er den tekniske realiseringen av nettverket gjort gjennom en nettverksentrikt tjeneste fra Norsk Helsenett (NHN). Nettverket tilrettelegger for integrasjon mellom nettverk i sky og lokale nettverkssoner gjennom transport og nettverkssoner.

## 4.3 Orkestrering og automatisering

Nettverket tar i bruk orkestrering og automasjon for å sikre mer effektiv drift og forvaltning, og skal realisere gevinster for helseforetakene og Sykehuspartner.

Sykehuspartner har etablert et eget sentralt IaC-miljø som jobber med automasjon av nettverket. Dette baseres på infrastruktur som kode (IaC).

IaC-utviklerplattformen benytter API-er publisert og tilgjengeliggjort fra nettverks- og sikkerhetkontrollere lokalisert i henholdsvis helseforetakene og de sentrale datasentrene, for å gjennomføre automatisering av nettverk og nettverkskomponenter.



Figur 2: Relasjonen mellom Sentralisert automasjon og grensesnitt i nettverket.

#### 4.3.1 Applikasjoner og programvare

Nettverks IaC utviklerplattformer bruker følgende programvare for å kunne utføre endringer på nettverkskontrollere fra servere:

- GitHub Actions Runner
- Python
- Terraform

#### 4.4 Overvåkning og nettverksdrift

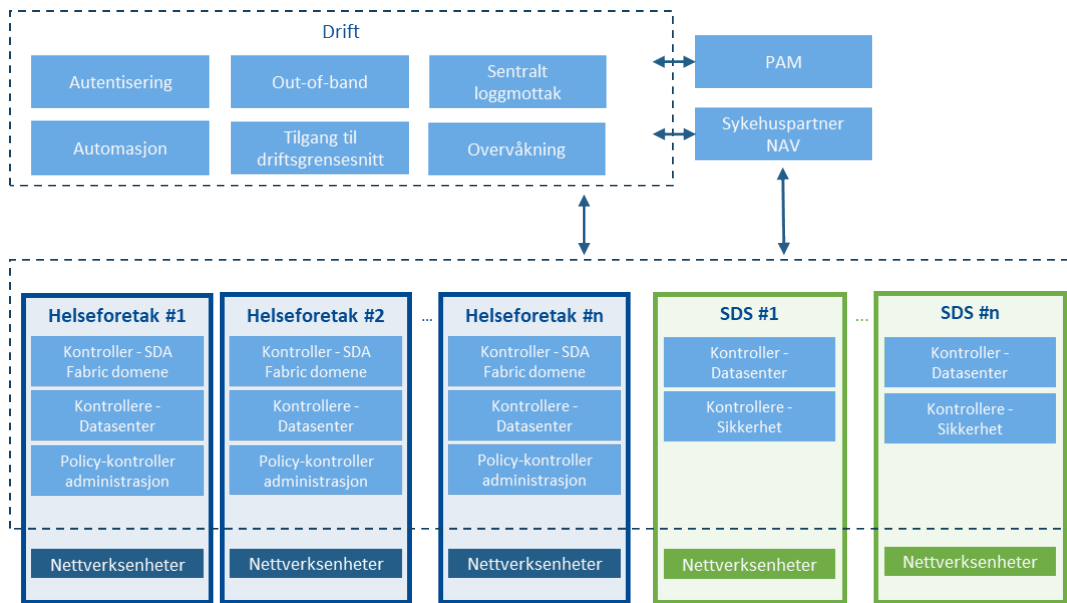
Nettverket skal sikre tilstrekkelig innsyn for privilegert drift- og sikkerhetspersonell, men skal også sikre datafangst innenfor nettverkshelse, utnyttelse, sikkerhet og bruker-/applikasjonsopplevelse.

DNA assurance (del av DNA center) vil gi Nettverket drift- og forvaltningsressurser i Helse Sør-Øst et maskinlæringssystem, som vil være et verktøy for å kunne rapportere filtrerte og presise data som anvendes for nettverksdrift.

Sykehuspartners operasjonssenter overvåker alarmer fra nettverksenheter og -kontrollere ved hjelp av maskinlæringssystemer som er innebygd i nettverkets kontrollere.

Sykehuspartners PAM-løsning benyttes for autentisering og tilgangsstyring med privilegert tilgang for å få tilgang til automasjonsløsninger for utføre feilsøking, konfigurasjon og administrasjon av nettverksenheter og nettverkets kontrollere.

Skissen under viser det overordnede prinsippet for overvåkning og drift:



Figur 3: Driftskonsept basert på kontrollere og automasjon

## 5 Ekstern aksess WAN

Ekstern aksess har funksjoner for å sikre interoperabilitet mellom Helse Sør-Østs lokasjoner. Dette sikrer kontroll over intertrafikk i Helse Sør-Øst, samtidig som det sikrer trafikk til og fra eksterne soner i regionen.

Funksjoner i ekstern aksess:

- Kjernenett fra Norsk Helsenett
- Virtualisering av transportnettverk gjennom Carrier Supporting Carrier (CsC)
- Transportnett og tilkoblingsmodeller for Virtuelle nett (VN)
- WAN tilknytningspunkt (WTP) for SDS inkludert CsC funksjonalitet
- Regional ekstern aksess, realisert i SDS, for sentralisert brannmur funksjonalitet mellom transportsoner og eksterne soner
- Tilkobling av eksterne nettverk til Helse Sør-Østs nettverk gjennom front-end rutere



Figur 4: Funksjoner i Ekstern Aksess

## 5.1 Stamnett fra Norsk Helsenett

Alle lokasjoner i Helse Sør-Øst tilknyttes Norsk Helsenetts nasjonale stamnett. Stamnettet leverer krypterte føringsveier til alle foretak i HSØ, med tilstrekkelig redundans, diversitet og kapasitet.

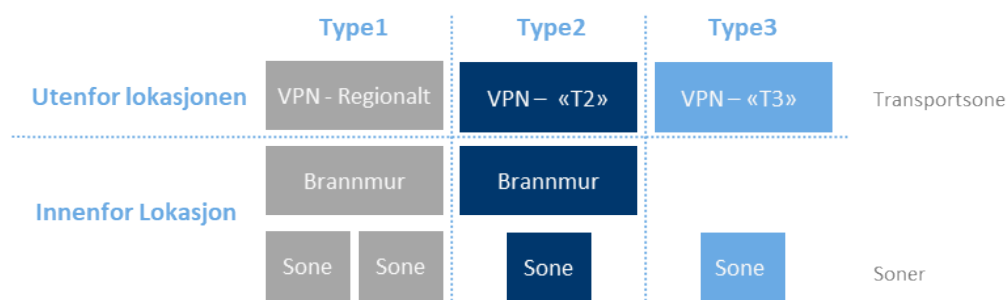
Carrier supporting carrier (CsC) er en løsning man bruker for levere tjenester gjennom en hovedoperatør, som i dette eksempelet er Norsk Helsenett, mens støtteoperatør er Sykehuspartner. CsC benyttes for å transportere tjenester over lange eller korte avstander, uten av Sykehuspartner trenger å lage noen infrastruktur imellom. Norsk Helsenett utvikler, drift og forvalter digital infrastruktur for HSØ.

## 5.2 Virtualiserte transportnettverk

Alle lokasjoner i Helse Sør-Øst skal være tilknyttet NHNs krypterte stamnett. For å få trafikk over transportnettverket til NHN, brukes CsC for å virtualisere Helse Sør-Østs spesifikke MPLS nettverk over transportnettverket til NHN. Helse Sør-Øst transporterer trafikk over CsC for følgende lokasjons kategorier: A++/A+/A/B, samt mot SDS.

## 5.3 Designmønstre for Transportsoner

Bruken av virtuelle transportnettverk er blitt standard, og det er etablert standard designmønstre for transportsoner i Helse Sør-Øst. Se figur7 nedenfor.



Figur 5: Designmønstre Type1, Type2 og Type 3 for Transportsoner

Det er lagt opp til tre standardiserte designmønstre i Helse Sør-Øst, som kort beskrevet nedenfor. Type 1 er den som dekker de fleste behov i nettverket og skal det skal strebes etter å benytte der det er hensiktsmessig.

- **Type1** – standard tilkoblingsmetode for soner på en lokasjon. Regional VPN benyttes som transportnett. Brannmur kontrollerer trafikk mellom soner og transportsonen. Type 1 etableres på A++, A+, A og B lokasjoner, samt HF-HUB. Det er kun en type 1 leveranse per lokasjon.

- **Type2** – benyttes der hvor soner som av sikkerhetsgrunnet og/eller funksjonelle behov ikke kan ta del i felles transport med øvrige type 1 nettverk. Ved etablering av type 2 kreves det et eget dedikert transportnett via egen instans på NHN utstyr. Ved bruk av type 2, skal det etableres en lokal brannmurinstans på lokasjon som skal være separert fra Type 1.
- **Type3** – benyttes for soner som ikke være en del av felles transportnettverk, som type 1, type 2 eller benytte samme brannmurinstans som type 1 og 2 eller andre soner i type 3. Der hvor type 3 blir valgt som tilkoblingsmetode, skal hver sone være sitt eget transport nett. Type 3 trenger ingen lokal brannmur da dette er dedikerte transportnett for hver sone.

## 5.4 Tilknytningspunkt for WAN (WTP)

WTP er en funksjon for å sammenkoble Helse Sør-Østs virtualiserte transportnettverk, CsC, og de forskjellige modulene i de sentrale datasenter. WTP sørger for terminering av forbindelser fra NHN for regionalt bruk og interkommunikasjon mellom SDS-ene, samt knytningen mellom Datasenter nettverk og regional ekstern aksess per SDS.

## 5.5 Regional ekstern aksess

Regional Ekstern Aksess benyttes for å kontrollere trafikk mellom transportsoner og mellom transportsoner og eksterne nettverk. En brannmur instans i Regional Ekstern Aksess har grensesnitt til en eller flere transportsoner og/eller et eller flere eksterne nettverk.

I tillegg til brannmuren inkluderer Regional Ekstern Aksess nettverksenheter for tilkobling av eksterne nettverk:

- IPSecenhet - site-2-site IPsec basert VPN
- VPNKonsentrator - brukerbasert fjerntilgang med VPN-klient

Regional Ekstern Aksess realiseres i egne selvstendige sikkerhetskomponenter. Disse sikkerhetskomponentene utgjør perimetersikringen for Helse Sør-Øst. Det etableres flere brannmur-instanser for å realisere ulike kommunikasjonsbehov.

IPSec funksjonen inkluderer både krypterte forbindelser mot eksterne organisasjoner og for egne løsninger som er tilknyttet offentlig nett på eksterne lokasjoner. Fjerntilgang for interne brukere etableres uavhengig av IPSec funksjonen, og inkluderer VPN-klient-basert tilgang for administrerte klienter som er koblet til eksterne nett.

## 6 Eksterne nettverk

Ekstern aksess er ikke å anse som en del av Helse Sør-Østs interne nettverk, dette er internett, helsenett eller andre nettverk. Regional ekstern aksess som er en NHN-tjeneste har funksjonalitet for å sikre at det etableres nødvendige fysiske og logiske tilkoblinger, samt separasjoner mellom eksterne nettverk og Helse Sør-Øst interne nettverk.



Det skal etterstrebes som en standard, at alle eksterne nettverk skal termineres mot regional ekstern aksess, unntaket for standarden er å ha en godkjent risikovurdering for å etablere dette i interne transportsoner hvor man ser at det er behov.

## 6.1 Publisering av tjenester - DMZ

DMZ fungerer som et frontlinjenettverk som samhandler direkte med eksterne nettverk, samtidig som det logisk skilles fra det interne Helse Sør-Øst nettverket. Alle tjenester i Sykehuspartner som eksponeres mot eksterne lokasjoner, skal eksponeres via DMZ.

## 7 HF-LAN og lokalt datasenter

Hvert helseforetaks nettverk er modulært og har tatt i bruk forskjellige designmønstre til de ulike lokasjonsklassene. Helseforetakenes HF-HUB og lokasjonenes nettverk er bygget opp med følgende tjenester

- NHN Stamnett eller NHN SD-WAN som bærer av trafikk
- Fusion for virtualisering av transportnettverk gjennom Carrier supporting carrier (CsC) og sammenkobling av enheter
- HF-HUB for sentraliserte managementsystemer tilhørende helseforetaket
- Software Defined Access (SDA Fabric) for helseforetakets programvaredefinerte nettverk
- Lokasjonsbrannmur for filtrering av trafikk mellom soner og transportsoner
- Lokalt datasenter (LDS)
- Nettverk for IKT-rom med behov for server tilpasset nettverk (LTSN)

### 7.1 Klassifisering av lokasjoner

I henhold til målarkitekturen har HSØ delt inn sine lokasjoner i lokasjonsklassene A++, A+, A, B, C og D.

Lokasjonene kategoriseres basert på lokasjonens kritikalitet, skalering, lokal overlevelse og autonomi.

Kategori	Beskrivelse	Egenskaper
A++	Større sykehusområde med traumesenter og nasjonalt beredskapssenter	Trippel redundans i tilkobling til Stamnett med full diversitet. 3x100G tilkobling Stamnett. Lokal overlevelse og autonomi for kritiske nettverkstjenester Borderswitch, Intermediateswitch, Edgeswitch, trådløs kontroller, Fusion, lokal brannmur, samt ISE er etablert trippel redundant.
A+	Større sykehusområde	Redundant tilkobling til Stamnett (2x) med full diversitet * 3x100G tilkobling til kjerneswitch til Stamnett for stand-by-link * Lokal overlevelse og autonomi for kritiske nettverkstjenester Borderswitch, Intermediateswitch, Edgeswitch, trådløs kontroller, Fusion, lokal brannmur, samt ISE er etablert redundant.
A	Sykehus, sykehusområde	Redundant tilkobling til Stamnett (2x) med full diversitet 2x 10G – 100G tilkobling til Stamnett Lokal overlevelse og autonomi for kritiske nettverkstjenester.

		Borderswitch, Intermediateswitch, Edgeswitch, trådløs kontroller, Fusion, lokal brannmur, samt ISE er etablert redundant.
<b>B</b>	Lokalsykehus, medium og/eller kritisk lokasjon som innehar spesialfunksjon	Redundant tilkobling til Stamnett (2x) med full diversitet 2x 1G – 10G tilkobling til Stamnett Begrenset lokal overlevelse og autonomi for kritiske nettverkstjenester. Borderswitch, Intermediateswitch, Edgeswitch, trådløs kontroller, Fusion, lokal brannmur, samt ISE er etablert redundant.
<b>C</b>	Mindre, ikke-kritisk lokasjon	Ikke redundant tilkoblet Stamnett. Redundans kan etableres ved behov. 1x 100Mbps - 1Gbps tilkobling til Stamnett over SD-WAN Ingen lokal autonomi/overlevelse. Nettverket er ikke etablert redundant.
<b>D</b>	Mobil lokasjon	Ikke-redundant tilkoblet Stamnett. 1x mobil tilkobling til Stamnett SD-WAN, 4G (/5G) Opsjon for trådløst aksesspunkt og kablet nettverk, utover tilbudt løsning fra NHN.
<b>SDS</b>	Sentrale datasenter	Trippel redundans i tilkobling til NHN med full diversitet. Lokal overlevelse og autonomi for kritiske nettverkstjenester. Redundant Wan-TilknytningsPunkt for sammenkobling av eksterne soner og datasenterets lokale moduler.

Tabell 1: Lokasjonsklassifisering i henhold til Målbilde for Nettverk

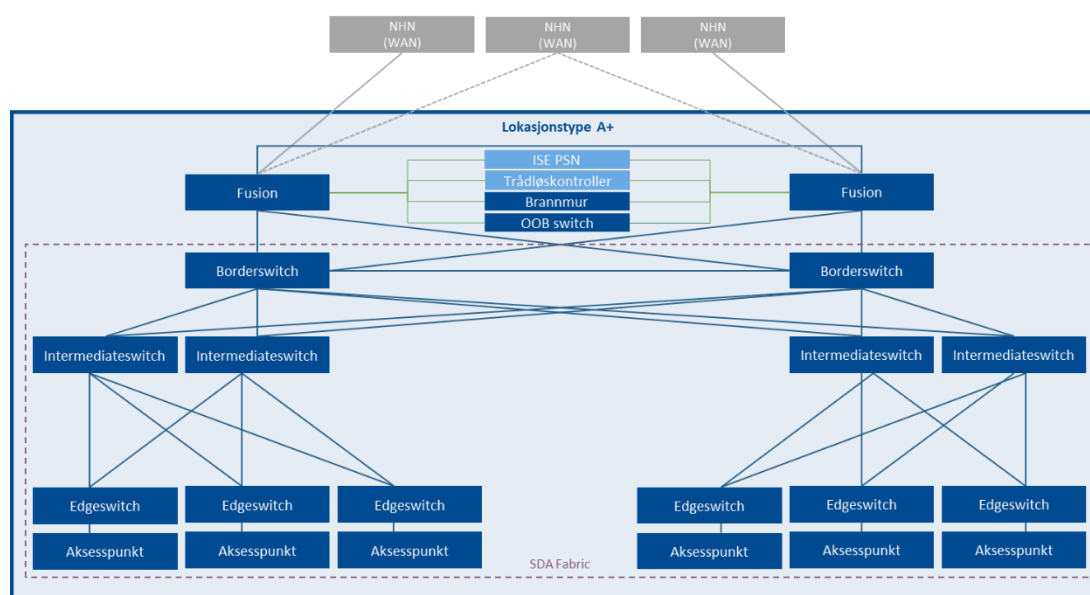
\* Lokasjonsklasse A+ er definert som en A-lokasjon med en ekstra WAN-forbindelse trukket inn i den ene kjernesvitsjen til bruk for stand-by. A+ vil ikke gi noe ekstra kapabilitet sett fra datasenter i forhold til opptid og feiltoleranse

## 7.2 Lokasjoner

Helseregionens lokasjoner er inndelt lokasjonsklasser, A++, A+, A, B, C og D

### Lokasjonsklasse A+ og A++

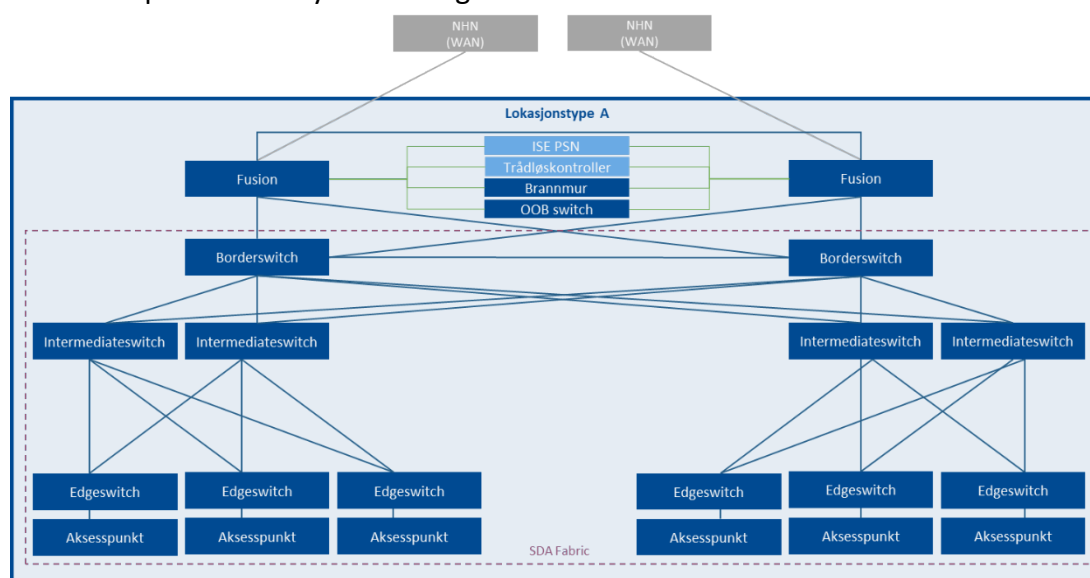
- Lokasjonsklasse A+ benytter trippelredundante forbindelser til NHN. Lokasjonsklassen inkluderer Fusion og SDA Fabric. Fusion er realisert redundant og gir tilkobling til ISE, trådløse kontrollere og lokal brannmur.
- SDA Fabric er etablert med to redundante Borderswitcher. Hver Intermediateswitch kobles mot to Borderswitcher. Det benyttes Intermediateswitcher for å koble sammen flere Edgeswitcher i ett aggregeringsnivå. En Edgeswitch tilknyttes to Intermediateswitcher. Aksesspunkter tilknyttes en Edgeswitch.



Figur 6: Overordnet skisse for Lokasjonsklasse A+

## Lokasjonsklasse A

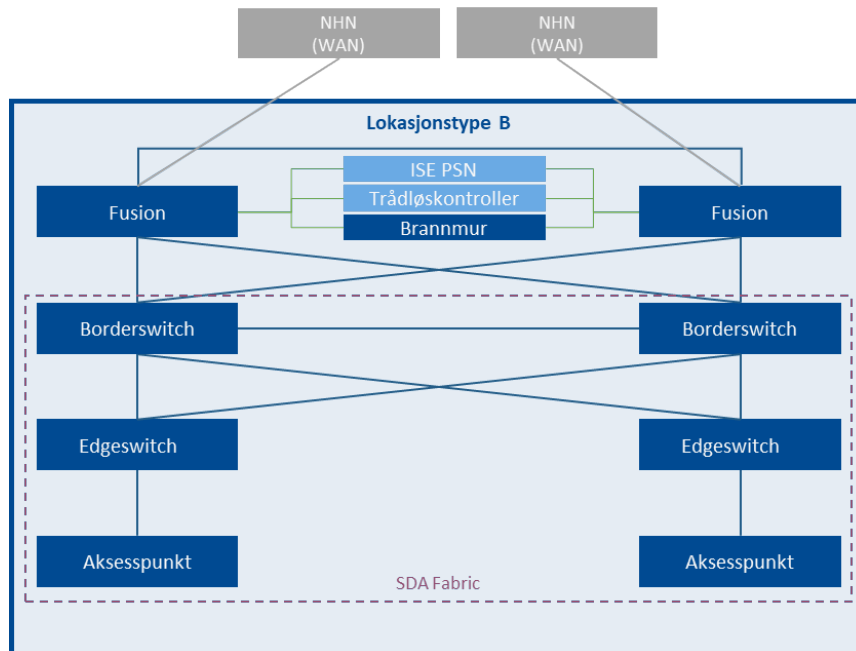
- Lokasjonsklasse A benytter redundant forbindelse til NHN. Lokasjonsklassen inkluderer Fusion og SDA Fabric. Fusion er realisert redundant og gir tilkobling til ISE, trådløse kontrollere og lokal brannmur.
- SDA Fabric er etablert med to redundante Borderswitcher. Hver Intermediateswitch kobles mot to Borderswitcher. Det benyttes Intermediateswitcher for å koble sammen flere Edgeswitcher i ett aggregeringsnivå. En Edgeswitch tilknyttes to Intermediateswitcher. Aksesspunkter tilknyttes en Edgeswitch.



Figur 7: Overordnet skisse for Lokasjonsklasse A

## Lokasjonsklasse B

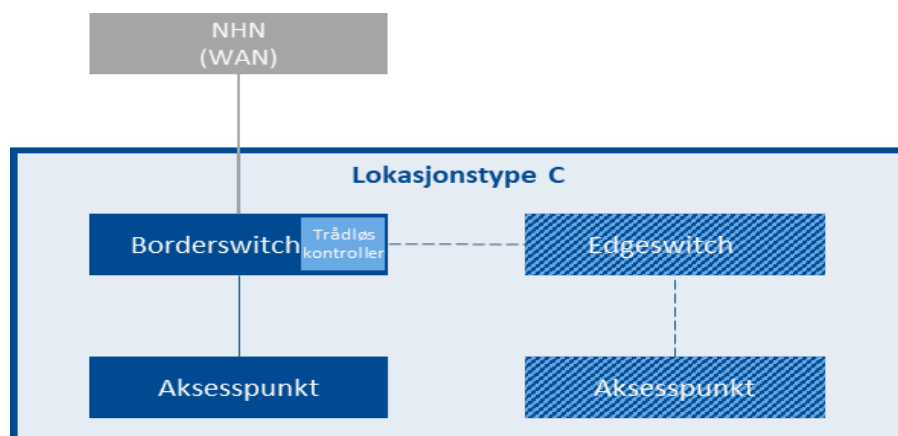
- Lokasjonsklasse B benytter redundant forbindelse til NHN. Lokasjonsklassen inkluderer Fusion og SDA Fabric. Fusion er realisert redundant og gir tilkobling til ISE, trådløse kontrollere og lokal brannmur.
- SDA Fabric er etablert med to redundante Borderswitcher. Edgeswitchene tilknyttes begge Borderswitchene. Aksesspunkter tilknyttes en Edgeswitch.



Figur 8: Overordnet skisse for Lokasjonsklasse B

### Lokasjonsklasse C

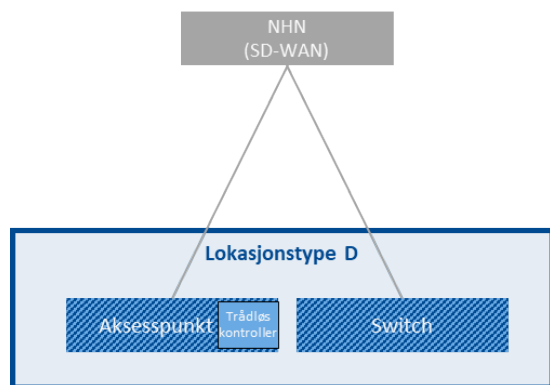
- Lokasjonsklasse C benytter SDA Fabric og en WAN -forbindelse basert på NHN SDWAN. SDWAN-forbindelsen kan alternativt tilby redundans.
- SDA Fabric består på en C-lokasjon minst av en Borderswitch som også kan operere som en Edgeswitch, altså tillater tilknytting av endepunkter. Løsningen kan utvides med flere Edgeswitcher, men det etableres i utgangspunktet ikke redundante forbindelser for disse. Lokasjonsklassen utstyres med et eller flere aksesspunkter. Borderswitchen har en innebygd trådløskontroller for kontroll med aksesspunkter.
- C-lokasjon har ikke egen Lokasjonsbrannmur, men benytter sentral brannmur i Helseforetakets HF HUB. SDA Fabric på C-lokasjoner tilhørende samme Helseforetak knyttes sammen og mot HF HUB basert på SDA Transit.



Figur 9: Overordnet skisse for Lokasjonsklasse C

### Lokasjonsklasse D

Lokasjonsklasse D består av en forbindelse til NHN, realisert gjennom NHN sin SD-WAN tjeneste. I tillegg kan det etableres trådløse aksesspunkter eller svitsjer som er underlagt nettverkets sentrale kontrollere. Men i utgangspunktet realiseres nettverket på en D-lokasjon direkte med leveransen fra NHN. Dette betyr at nettverket på lokasjonsklasse D ikke er etablert som en SDA Fabric eller deltar i Helseforetakets SDA Fabric, og således ikke støtter mikrosegmentering via SGT.

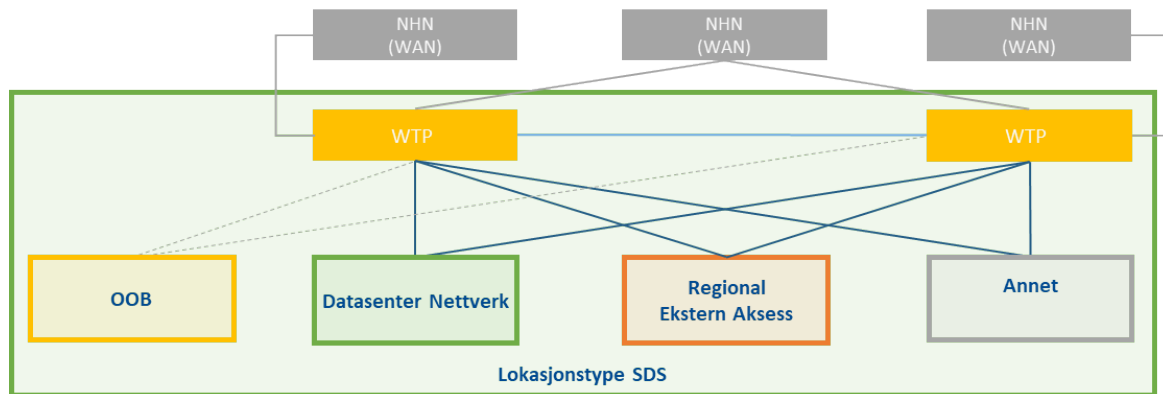


Figur 10: Overordnet skisse for Lokasjonsklasse D

### Lokasjonsklasse SDS

- I Målarkitektur for Nettverk er SDS klassifisert som lokasjonsklasse A++. I dette designet har man valgt å definere SDS som en egen lokasjonstype, da nettverkets funksjoner er forskjellige mellom de sentrale datasentrene og A+ lokasjonene.
- Lokasjonstypen SDS benyttes for lokalisering av ulike sentraliserte moduler:
  - Datasenter Nettverk
  - Out-of-Band (OOB)
  - Regional Ekstern Aksess

- Andre tjenester som ikke direkte inngår i dette designet, for eksempel ulike test/staging-miljøer, tredjeparts infrastruktur (on-premise skytjenester), etc.
- WanTilknytningsPunkt (WTP) knytter de ulike modulene sammen og består av redundante rutere som terminerer forbindelsene fra NHN de definerte modulene.



Figur 11: Lokasjonstype SDS med tilknyttede moduler

### Moduler knyttet til de forskjellige lokasjonsklassene

Utover de standardiserte lokasjonsklassene inkluderer designet også andre moduler. Dette er typisk nettverksfunksjoner som er samlokalisert med en av standard lokasjonsklassene. Tabellen under lister disse:

Kategori	Beskrivelse	Egenskaper
HF-HUB	Helseforetakets sentraliserte nettverksutstyr.	Realiseres på en A++, A+ eller A lokasjon.
Datasenter Nettverk	Sentralisert datasenter nettverk og brannmur for tjenesteproduksjon	Realiseres på en SDS-lokasjon.
Regional Ekstern aksess	Sikkerhetsfunksjon for kontroll og inspeksjon av trafikk for HSØ mot eksterne nettverk.	Realiseres på en SDS-lokasjon.
LDS	Helseforetakets lokale datasenter nettverk.	Realiseres på en A++, A+ eller A lokasjon.
LTSN	Helseforetakets lokale IKT-rom med behov for tilpasset servernettverk.	Realiseres på en A++, A+ eller A lokasjon.

Tabell 2: Lokasjons moduler

## 7.3 Seperasjon mellom helseforetakene

Nettverket skal administreres og håndteres sentralt i Sykehuspartner, men hvert feil- og sikkerhetsdomene er etablert slik at det ikke oppstår uønskede hendelser som vil påvirke nettverket i andre helseforetak. Dette unngås ved at hvert helseforetak er definert som egne administrative områder i CsC strukturen i HSØ. Gevinsten av dette gir en mer effektiv drift og

forvaltning som legger opp til bruk av automatisering av struktur og utrulling av policy for flere helseforetak.



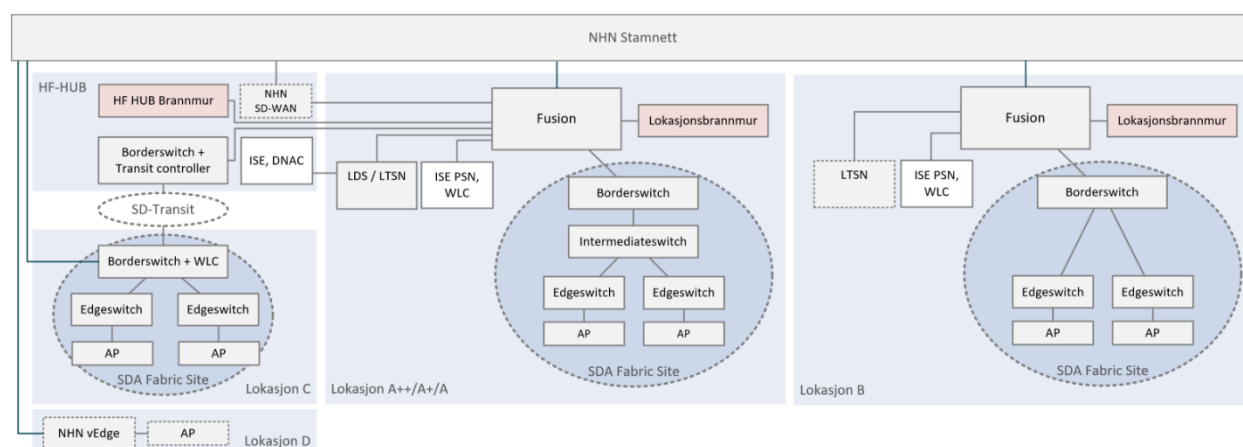
Figur 12: Separate administrative domener under en felles standardarkitektur og regional policy

Hvert helseforetak blir etablert med et nettverk basert på Cisco Software defined Access (SDA). Helseforetaket har sitt eget SDA Fabric domene og kontrollsystem.

SDA Fabric er tilknyttet tilgangs- og policykontrollere som er administrert per helseforetak eller lokasjon. Helseforetakenes lokasjoner settes opp som egne sikkerhetssoner, med selvstendige brannmurer som inngår i helseforetakets nettverk. Skulle en lokasjon ha behov for eget datasenternettverk vil dette også inngå i helseforetakets nettverk.

Kontrollsystemene i helseforetaket står for styring og kontroll i nettverket. Det er etablert tilgangskontroll på nettverket ved bruk av helseforetakets policykontrollere gjennom bruk av ISE for godkjenning av enheter som skal kobles til nettverket.

Ved behov for datasenternettverk på lokasjoner, skal det etableres ett programvaredefinert datasenternettverk ved bruk av en APIC kontroller for eget datasenter.



Figur 13: Overordnet skisse av lokalnett på et Helseforetak

Hovedpunkter ved figur:

1. Cisco Software Defined Network (SDA) benyttes som aksessnettløsning
2. NHN Stamnett benyttes som WAN mellom lokasjoner
3. Hver type A++, A+, A og B og C lokasjon etableres som en egen SDA Fabric Site
4. «Fusion» benyttes for å knytte Fabric Site sammen med øvrige komponenter per lokasjon
5. Hvert helseforetak har egne nettverks- og policykontrollere (DNAC, ISE) plassert i HF-HUB.

Løsningen dekker de definerte lokasjonsklassene A++, A+, A, B, C og D.

## 7.4 Felles kontrollsystemer for Helseforetakets lokalnett (HF-HUB)

Hvert helseforetak har behov for sentrale kontrollsystemer, dette kalles HF-HUB og er fysisk lokalisert på en av helseforetakets lokasjoner.

Alle helseforetak kan ha behov for flere IKT-rom med datasenternettverk. Lokalisering av HF-HUB krever at lokasjonen har datasenternettverk tilgjengelig for å kunne etablere de kontrollerfunksjonene en HF-HUB innebærer.

Ved etablering av HF-HUB skal standardiseringen og den logiske modellen som er lagt opp i designet i modernisert nett følges.

## 7.5 Brannmur på lokasjonene

Isolasjon mellom Helseforetak realiseres gjennom at det etableres lokasjonsspesifikke soner i lokasjonenes nettverk. Dette bidrar til å sikre Helseforetakets data og endepunkter, samt beskyttelse mot at sikkerhetshendelser forplanter seg fra et Helseforetak til et annet. Kommunikasjon mellom soner kontrolleres i en brannmur.

Det er etablert en lokal brannmur for lokasjonsklassene A++/A+/A/B. Løsningen støtter instansiering av virtuelle brannmurer. Dette støtter lokasjonens behov for de forskjellige sonenes på lokasjonens tilkobling til ulike transportnett. IDS funksjonalitet er aktivert på brannmuren på Helseforetakenes A++/A+/A/B lokasjoner.

C og D-lokasjoner har ikke egen lokasjonsbrannmur. De benytter brannmur på Helseforetakets HF HUB for kontroll av trafikk mellom soner og mot transportnett. C-lokasjoner benytter SDA Transit for å strekke sine soner til Helseforetakets HF HUB. D-lokasjoner benytter NHN SDWAN for tilsvarende funksjonalitet.

## 7.6 Policybasert tilgangskontroll

Endepunkter som knyttes til nettverket på Helseforetaket skal autentiseres før de gis tilgang. Dette skjer primært gjennom bruk av IEEE 802.1x og sertifikatbasert autentisering (EAP-TLS).

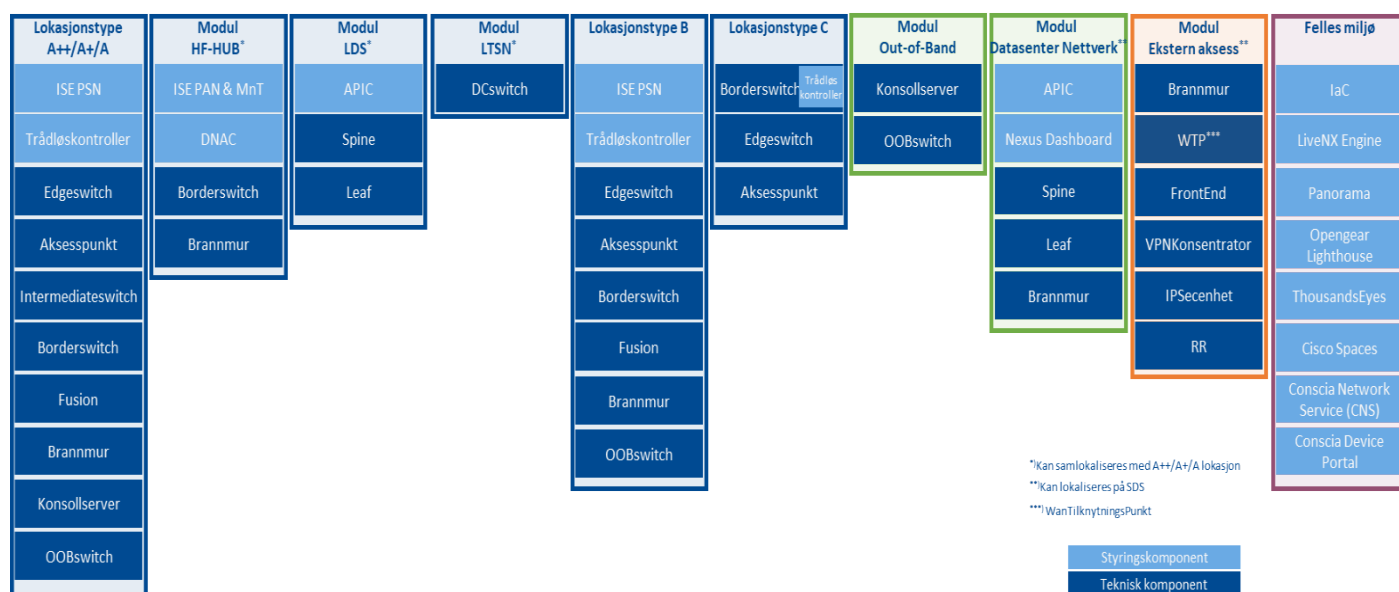


Ikke alle endepunkter i nettverket støtter 802.1x. For disse benyttes en kombinasjon av profilering av endepunktet og validering av endepunktets MAC-adresse mot en liste av godkjente enheter (Mac Address Bypass (MAB)).

Basert på autentisering tilknyttes endepunktet en sone, IP-subnett og mikrosone basert på definert policy. Løsningen håndhever policy for tilgang internt i en mikrosone og mellom mikrosoner. Policyen er spesifikk for hvert enkelt helseforetak, men er bygd etter en førende mal fra regional policy slik at helseforetakene gis et felles regionalt sikkerhetsnivå.

## 7.7 Komponenttyper

Den overordnede løsningsarkitekturen er brutt ned i forskjellige komponenter, der noen komponenter gjenbrukes mellom forskjellige lokasjonsklasser. Figuren og tabellen under, skisserer de forskjellige komponenttypene som benyttes. Alle lokasjoner kommer ikke til å benytte seg av alle komponenttyper.



Figur 14: Komponenter per lokasjonsklasse og modulkategori

Modul	Lokalisering	Detaljert
ISE PSN	Lokasjonsklasse A++/A+/A/B	Lokal Policy-kontroller for Helseforetakets lokasjonsklasser A++/A+/A/B. Policy Service Node (PSN) er funksjonen som benyttes for autentisering av endepunkter fra Aksesspunkter og Edgeswitch.
Trådløskontroller	Lokasjonsklasse A++/A+/A/B/C	Enhet for administrasjon av aksesspunkt. Kan også leveres integrert i en Borderswitch.
Edgeswitch	Lokasjonsklasse A++/A+/A/B/C	Svitsj for tilknytning av endepunkter eller andre svitsjer

Modul	Lokalisering	Detaljer
Aksesspunkt	Lokasjonsklasse A++/A+/A/B/C	Trådløstaksesspunkt for tilknytning av endepunkter
Intermediateswitch	Lokasjonsklasse A++/A+/A/B	Svitsjer for tilknytning av andre svitsjer
Borderswitch	Lokasjonsklasse A++/A+/A/B/C	Svitsjer for håndteringen av SDA Fabric.
Fusion	Lokasjonsklasse A++/A+/A/B	Svitsjer for sammenkobling av komponenter av modulene på en lokasjon. Se for øvrig avsnitt <b>Error! Reference source not found..</b>
Brannmur	HF-HUB, Sentrale datasentre, Regional Ekstern Aksess, Lokasjonsklasse A++/A+/A/B	Kontrollpunkt for nettverkstrafikk.
Konsollserver	HF-HUB, Sentrale datasentre, Lokasjonsklasse A++/A+/A/B	Out-Of-Band enhet der administrasjonsgrensesnitt for endepunkter, servere eller datasentre utstyr kan tilkobles.
OOBswitch	Lokasjonsklasse A++/A+/A/B, Sentrale datasentre	Dedikerte svitsjer for tilkobling av Ethernet baserte administrasjonsgrensesnitt.
ISE PAN & MnT	HF-HUB	Sentralisert Policy-kontroller per Helseforetak. Ivaretar sentralisert konfigurasjon og styring av lokale Policy-kontrollere
DNAC	Orkestrering og automatisering	Kontroller for Helseforetakets programvaredefinert nettverk.
APIC	Sentrale datasentre, lokale IKT-rom med behov for datasentre nettverk	Application Policy Infrastructure Controller (APIC) som benyttes til kontroll av konfigurasjonen i Spine og Leaf.
Spine	Sentrale datasentre, lokale IKT-rom med behov for datasentre nettverk	Datasenterswitch for sammenkobling av flere Leaf
Leaf	Sentrale datasentre, lokale IKT-rom med behov for datasentre nettverk	Datasenterswitch for tilknytting av servere og datasentre utstyr
WanTilknytningsPunkt	Sentrale datasentre	Ruter for sammenkobling av komponenter av modulene på SDS.
RR	Sentrale datasentre	Rutere, Route Reflector, som kjører BGP prosesser for utveksling av routing i CsC.
DCswitch	Regional Ekstern aksess, Lokasjonsklasse A++/A+/A med lokale IKT-rom med behov for tilpasset server nettverk	Svitsj for konfigurasjon av Lag 2 domener for datasentre. Er adskilt fra resterende infrastruktur via lag 3.
FrontEnd	Sentrale datasentre	Ruter for håndtering av BGP-peering mot eksterne nettverk
IPsecenhet	Regional Ekstern aksess	Enhet for terminering av IPsec baserte Lan-to-Lan VPN tuneller
VPNkonsentrator	Regional Ekstern aksess	Enhet for terminering av bruker baserte VPN tuneller
IaC miljø	Fellesmiljø	IaC miljø består av systemene som spiller sammen for å realisere kode mot infrastruktur og inkludere blant annet utvikler miljø, VCS og CI/CD.
Live NX	Fellesmiljø	Analyseverktøy for Netflow data
OpenGear Lighthouse	Fellesmiljø	Administrasjonssystem for OOB funksjonen.
ThousandEyes	Fellesmiljø	Plattform for måling av tjenestekvalitet.
Panorama	Fellesmiljø	Sentralisert administrasjonspunkt for brannmur administrasjon
Cisco Spaces	Fellesmiljø	Plattform for lokasjonstjenester.
Conscia Device Portal	Fellesmiljø	Administrasjons portal for IoT enheter.

Modul	Lokalisering	Detaljert
Conscia Network Services	Fellesmiljø	Plattform for livsyklusadministrasjon

Tabell 3: Beskrivelse av komponent typer

## 7.8 Lokal Datasenterfunksjon

Lokasjoner som har særskilt behov for lokal prosessering av datatjenester, tilbys to varianter for datasenterfunksjonalitet:

- LTSN - Lokalt tilpasset Server Nettverk
- LDS – Lokalt Datasenter Nettverk

LTSN tilbys på lokasjoner hvor behovet for lokal serverkapasitet er beskjedent, og ikke har behov for et komplett datasenter infrastruktur. LTSN gir mulighet for standard servertilknytning i rack, fordelt på ett eller to sentrale hovedkommunikasjonsrom (xHKR).

LDS tilbys på lokasjoner der behovet for lokal serverkapasitet er betydelig, eller spesielt kritisk. Denne varianten leverer et komplett datasenter infrastruktur, og understøtter automatisert provisjonering, mikrosegmentering og monitorering.

For begge varianter er det et krav at soner for servertjenestene følger kravene i «NO-43 Sikkerhetspolicy for regional sonemodell»

### 7.8.1 Lokalt tilpasset Server Nettverk

Lokalt tilpasset server nettverk (LTSN) består av et redundant Lag-2-basert nettverk for tilknytning av server-ressurser på datarom.

LTSN modulen tilknyttes Fusion node på aktuell lokasjon, og Fusion fungerer som ruter og lokal gateway i de ulike server-segmentene tilknyttet LTSN. Sonene som tilhører LTSN, kontrolleres av Lokasjonsbrannmuren på tilhørende lokasjon.

### 7.8.2 Lokalt Datasenter Nettverk

Lokalt Datasenter nettverk (LDS) benytter programvaredefinert nettverk, og bygges etter tilsvarende design fra Datasenter Nettverk i sentrale datasentre (SDS) med tilsvarende kapabiliteter. Løsningen baseres på Cisco ACI og inkluderer dedikerte brannmurer for datasenterfunksjonen.

LDS gir lokal autonomi og robusthet, selv med bortfall av tjenester fra de sentrale datasentrene eller andre Helseforetak. LDS er bygget for kontinuerlig videresending av trafikk, selv ved bortfall av nettverkskontrolleren for LDS - APIC. LDS modul tilknyttes Fusion node på aktuell lokasjon.

### 7.8.3 Applikasjonslastdeling (ADC)

For lokasjoner med lokal datasenterfunksjon (LTSN/LDS), tilbys mulighet for lastdeling av tjenester dersom det er behov for dette. Lastdelingsfunksjonen gir blant annet følgende fordeler:

- **Optimal utnyttelse av ressurser:** Lastdeling distribuerer trafikken jevnt over flere servere, noe som bidrar til å forhindre overbelastning av noen få servere og sikre best mulig bruk av tilgjengelige ressurser.
- **Reduksjon av ventetid:** Ved å fordele belastningen kan lastbalanserer rute forespørsler til servere med lav belastning, noe som reduserer responstiden og ventetiden for brukerne.
- **Feiltoleranse:** Hvis en server feiler, kan lastbalanseren automatisk om dirigere trafikken til de gjenværende fungerende serverne, slik at tjenesten opprettholdes med minimale forstyrrelser.
- **Høy tilgjengelighet:** Ved å fordele trafikken over flere servere, blir systemet mindre sannsynlig å oppleve nedetid på grunn av en enkelt serverfeil.
- **Høy skalerbarhet:** Lastbalansering gjør det enklere å skalere systemet ved å legge til flere servere etter behov. Dette gjør det mulig å håndtere økt trafikk uten å påvirke ytelsen eller tilgjengeligheten.
- **Sikkerhet:** Distribuert belastning forhindrer overbelastningsangrep. Lastdeling kan bidra til å beskytte mot distribuerte tjenestenektangrep (DDoS) ved å spre trafikken over flere servere, noe som gjør det vanskeligere for angripere å overbelaste en enkelt server.
- **Forenkler oppgraderinger og vedlikehold:** Når det er nødvendig med systemoppgraderinger eller vedlikehold, kan enkelte servere tas offline uten å påvirke tilgjengeligheten, da lastbalanseren vil rute trafikken til de gjenværende fungerende serverne.
- **Bedre brukeropplevelse:** Jevn fordeling av trafikken kan føre til raskere responstider, noe som forbedrer brukeropplevelsen.

I HSØ benyttes lastdelingsløsninger fra leverandøren Big-IP F5.

## 7.9 Tilgang til nettverksinfrastruktur via Out-Of-Band (OOB)

For å sikre tilgang til sentrale nettverksenheter er det etablert et eget fysisk separat Ethernet nettverk for Out-of-Band (OOB) på lokasjoner som har kritiske komponenter. Dette nettverket består av dedikerte OOB-switcher, og er tilkoblet lokasjonens Fusion node.

OOB nettverket benyttes også til management av andre enheter, som tilgang til IDRAC/ILO/CIMC grensesnitt. Det etableres egne subnett der det er behov for å skille denne trafikken fra nettverksenheter.

OOB gir også seriell konsolltilgang gjennom konsoll-serverne. Dette benyttes for direkte tilgang til enheter som har serieport for å sikre muligheter for feilsøking ved fysiske feil på utstyret, for overvåking av oppstartsprosesser, ved programvare oppgraderinger og omstart av kritisk utstyr.

I normal drift er OOB-tjenestene, nettverk og konsoll, tilgjengelig via det normale drifts-/administrasjonsnettverket. Ved feil på administrasjonsnettverket, kan OOB-tjenestene gjøres tilgjengelig for teknikere via en egen kryptert løsning over 4G/LTE. OOB-infrastrukturen

installeres utenfor produksjonsnettverket for å hindre at ett enkelt feilpunkt kan hindre tilgang til administrasjonsnettverket.

## 8 Trådløst nettverk

### 8.1 Generelt

Det trådløse nettet skal være sikkert, tilgjengelig, skalerbart og ha tilstrekkelig kapasitet og kvalitet. På den måten kan man sikre mobilitet og fleksibilitet til tjenestene som tilbys. For design og planlegging av det trådløse nettverk benyttes Ekahau Site Survey som verktøy. Ved hjelp av blant annet byggetegninger som viser tykkelse og materiale i vegger og tak, vil man komme frem til den best mulige plasseringen av trådløse aksesspunkter i et bygg. Kravene som blir brukt for designet er basert på dokumentasjonen til utstyr med høye krav til dekning, som IP Telefoni, RTLS og Telemetry.

### 8.2 Struktur

Designet for trådløst nett på et helseforetak bygger på regionale standarder i HSØ, samt beste praksis for trådløs infrastruktur. Arkitekturen benytter en laginndelt (SSID) struktur for å definere hvor de enkelte komponentene rutes i nettverket (VLAN) og hvilke funksjoner som befinner seg innenfor laget.

Designet er laget for å gi en redundant, stabil og skalerbar infrastruktur for klienter som kobler seg mot HF trådløse nettverk. Designet er bygd opp rundt Wireless LAN Controller (WLC) som kontrollerer alle aksesspunktene (AP) som befinner seg i helseforetakets nettverk.

### 8.3 Aksesspunkter

Aksesspunktene kobles til nærmeste kantsvitsj og skal ha minst 1 Gbps båndbredde tilgjengelig på porten. Punktene får strøm direkte fra svitsjen via PoE+ (Power over Ethernet). Dersom alle funksjoner i et aksesspunkt skal støttes, kan det være nødvendig med inntil 60W effekt på svitsjeport.

For å sikre at ikke hele dekningen i et område forsvinner dersom en kantsvitsj faller ut, fordeles aksesspunktene så langt det er mulig på flere svitsjer i et koblingsrom. Det bør også tilstrebes at to nabo-aksesspunkter ikke er koblet til samme svitsj.

Alle aksesspunkter skal ha støtte for 802.11ax/6E standarden som et minimum, samt være tilbakekompatible til 802.11a. Det bør tilstrebes at alle aksesspunkter på en lokasjon er av samme modell.

Trådløst nett integreres, som en del av SDA Fabric på de lokasjonstyper som benytter SDA. Den trådløse infrastrukturen bestående av APer og WLCer tar del i LISP/VXLAN-kontrollplanet. Denne konfigurasjonen benevnes som Fabric Enabled Wireless (FEW).

Med Point of Presence (PoP) menes det punktet i nettverket hvor trafikk fra trådløse klienter switches ut fra den logiske trådløse infrastrukturen og inn i den logiske kablede infrastrukturen. PoP er dermed det stedet i nettverket hvor IP-subnet for klienter er definert og som håndterer segmentering og videre ruting av trafikken.

Trafikk fra enheter knyttet mot det trådløse nettverket sendes fra et fabric AP til den Edgeswitch som AP er koblet. Trafikken er enkapsulert i VXLAN for å bevare segmentering og policy. PoP for klienten er SDA Edgeswitch. Dette følger Cisco sitt standard SDA-design.

Alle AP-er er plassert inn i bygningstegning per bygning > etasje i DNA Center. Der dette er tilgjengelig konfigureres informasjon om høyde over gulvet og antennens retning for å forbedre posisjonering.

AP i løsningen er tildelt site-tag og policy-tag automatisk av DNA Center og følger standard design for Fabric Enabled Wireless.

## 8.4 WLAN Kontrollere

WLAN kontrolleren er enheten som kontrollerer den trådløse infrastrukturen. All konfigurasjon og parametre på tilkobleaksesspunkter gjøres av kontrolleren. Det samme gjelder autentisering og håndtering av klienter. Nødvendig følge av Fabric Enabled Wireless benytter hver Fabric Site (lokasjon) egen lokal trådløs-kontroller.

Hvert sykehus med lokasjonsklassifisering A++, A+, A og B har to kontrollere i HA-SSO oppsett plassert i SHKR, og koblet til Bordersvitsjene. WLC-ene tilbyr Stateful Switch Over (SSO) for aksesspunktene i en feilsituasjon. Oppsettet benytter Redundancy Port (RP), Redundancy Management Interface (RMI) og Gateway Reachability Detection for replikering og deteksjon av dual-active-scenario.. aksesspunktdatabasen på den aktive WLC-en er replikert til den sekundære WLCen, og dette gjør det mulig med failover uten merkbart utfall, fordi den sekundære WLC-en allerede har informasjon om koblingene til alle aksesspunktene.

WLCene krever at både primær og sekundær server har samme maskinvare og programvare for at HA skal fungere. Lisenser blir arvet fra Primary WLC til Standby WLC.

## 8.5 Dekning

Alle lokasjoner som skal ha trådløs dekning, skal i utgangspunktet være heldekket. Dersom det ikke er et umiddelbart behov for dekning overalt, skal det likevel utføres en dekningsanalyse av hele bygget/ lokasjonen for å sikre riktig plassering av aksesspunkter i forhold til en eventuell fremtidig dekningsutvidelse.

En dekningsanalyse skal alltid utføres basert på kriterier for å sikre en tetthetsgrad av aksesspunkter som gir god kapasitet og tilgjengelighet. Slike kriterier kan være:

- 20 MHz kanalbåndbredde på sykehus. 40 MHz kanalbåndbredde benyttes på lokasjoner med rene administrative klienter.
- Ikke lavere signalstyrke (RSSI) enn -65dBm for Primær aksesspunkt i et dekningsområde.
- Ikke lavere signalstyrke (RSSI) enn -75dBm for Sekundær aksesspunkt i et dekningsområde.

Dette er noen av flere kriterier som er avgjørende for cellestørrelsen til et aksesspunkt. TPC (Transmit Power Control) som justerer omliggende aksesspunkters sendereffekt ved bortfall av et aksesspunkt, settes innenfor forhåndsdefinerte terskelverdier. Kanaler settes statisk.

## 8.6 Klient-VLAN for trådløse klienter

For WLAN med sentral svitsjing der det kan antas å bli flere enn 500 enheter som kobles til det samme WLAN, skal VLAN grupperes på kontroller (Interface Group, VLAN Pool, etc.) slik at den kan fordele klientene på flere mindre VLAN i stedet for et stort.

## 8.7 WLAN SSID

Et aksesspunkt kan ha opptil 16 forskjellige Service Set Identifiers (SSID), men av ytelsesmessige hensyn bør antallet begrenses så lang som mulig, og det er regionalt satt en øvre grense på åtte SSIDer per aksesspunkt, med en anbefalt grense på fire til seks.

Som standard blir det etablert fire SSIDer:

- «HSO Wireless» for klienter som kan autentiseres med 802.1x
- «HSO IoT» Komponent autentiseres ved bruk av PSK WPA2 eller via Radius mot AD og tildeler klient-vlan dynamisk avhengig av hva som returneres fra Radiusserveren.
- «HSO Gjest» for regionalt gjestenett (BYOD).
- «HSO Voice» for IP telefoner (I dag Ascom)
- «Eduroam» Gjestenett med autentisering gjennom EduRoam.

SSIDer i løsningen benytter standardene 802.11r(kun HSO voice), 802.11k og 802.11v for å optimalisere roamingen mellom AP. Klienter som roamer mellom AP på samme lokasjon har ikke behov for å endre IP-Adresse. I tillegg kan det være aktuelt å lage en særskilt SSID for klienter og utstyr som ikke kan bruke 802.1x eller av andre grunner bør skilles ut. Et eksempel på dette vil kunne være medisinsk-teknisk utstyr eller som krever rask og sømløs roaming og QoS-klassifisering som sikrer prioritet i eteren.

## 8.8 Sporing og lokalisering

Den trådløse infrastrukturen basert på Cisco aksesspunkter og Cisco trådløse kontrollere, gir sammen med Cisco Spaces et rammeverk for sporing og lokalisering i nettverket.



Den trådløse infrastrukturen kan rapportere posisjonsdata til Cisco Spaces gjennom tjenesten Cisco Spaces Connector. Cisco Spaces Connector er installert i SDS i Sikker sone, og fungerer som proxy mellom infrastrukturen og Cisco Spaces.

Løsningen støtter også sporing via Bluetooth Low Energy (BLE). Denne funksjonaliteten kan berikes av støttede tredjeparts løsninger.

## 8.9 Sikkerhet

De trådløse nettene sikres basert på type klienter og tjenester som skal nås. I utgangspunktet skal 802.1x benyttes for autentisering og VLAN-tildeling basert på gruppetilhørighet i Active Directory for brukeren. EAP-TLS brukes som autentiseringsmetode slik at maskin-/brukersertifikat kan benyttes.

For klienter som ikke støtter 802.1x, benyttes WPA2-PSK (Pre-shared Key) og eventuelt MAC-filtrering som kryptering og autentisering/autorisering.

## 9 Innendørs Mobildekning 4G/5G

Helseforetakene i HSØ skal ta i bruk og utnytte mobil arbeidsflate og moderne applikasjoner som verktøy for å understøtte effektiv pasientbehandling og sykehusdrift. For at Sykehuspartner skal kunne levere på dette behovet, er full trådløsdekning en forutsetning for at tjenester skal være stabile, sikre, heldekkende og sømløse. Flere og flere tjenester, administrative så vel som kliniske, forutsetter full trådløs dekning.

Mobildekning i er utfordrende i nyere bygg. Dette skyldes strengere miljøkrav til energisparing, som har ført til at byggene inneholder større mengder termisk isolasjon. Vegger inneholder metallisolerte materialer og vinduer består av flere lag glass og strålingsreflekterende metallfolie. Det vil forverres ytterligere når nye mobilteknologier som 5G tar i bruk høyere frekvenser som igjen er mer utsatt for demping. Dette vil resultere i at sykehuspersonell, besøkende og pasienter vil oppleve lav samtalekvalitet og dataoverføringer, man kan også komme over flere områder i bygget man ikke vil ha noen dekning. Dette kan være kritisk ved en nødsituasjon.

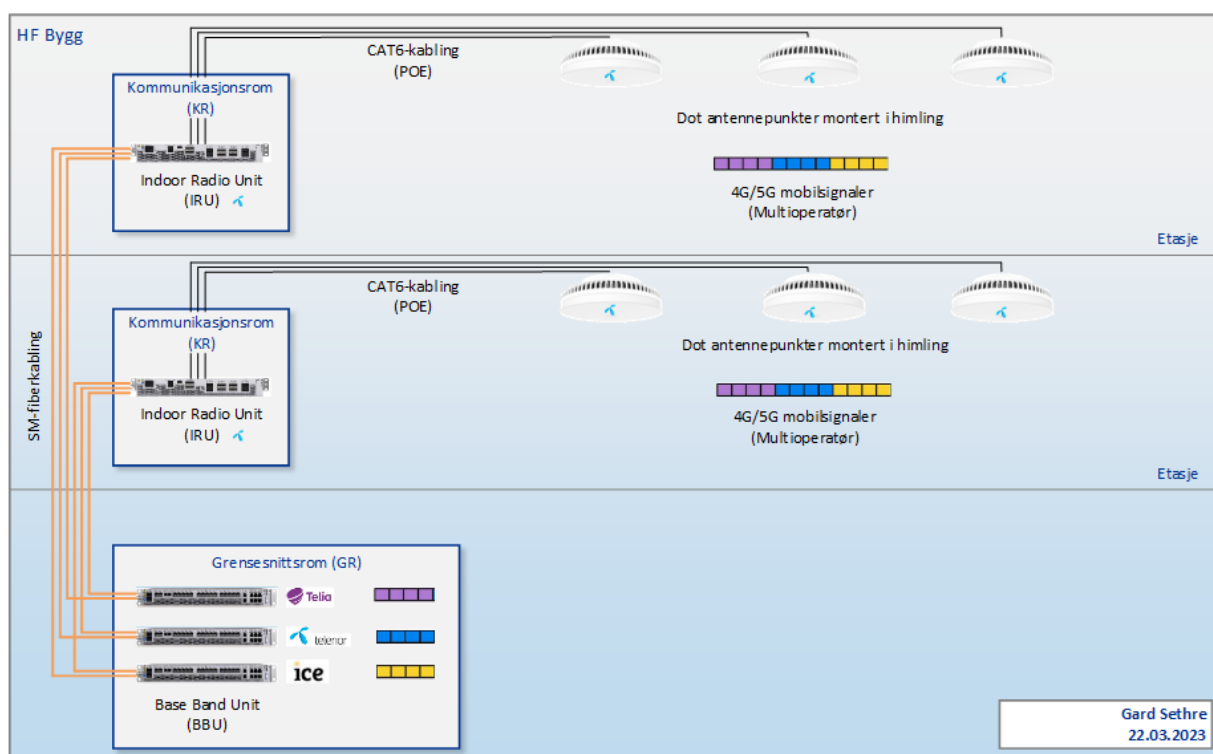
Heldekkende trådløst nett (Wifi) gjennomføres i dag som primærbærer for mobile applikasjoner i HSØ, inkludert varsel, tale og meldinger. Det skal i tillegg legges opp til heldekkende innendørs og utendørs 4G/5G mobildekning innenfor anviste sykehusområder hvor sykehuspersonell vil befinne seg.

Bakgrunnen for en sekundær bærerstrategi i HSØ er for å sikre kritiske trådløse/mobile tjenester, som telefoni, kritiske alarmer/varslinger/meldinger alltid skal komme frem til mottaker. Ved å ha to uavhengig bærere i og utenfor bygget, reduserer man sårbarheten og risikoen dersom en mobil arbeidsflate beveger seg utenfor et område hvor det ikke er dekning for en av bærerne, eller dersom en av bærertjenestene faller ut. Full dekning av begge bærere betyr at man vil ha høyere oppetid og stabilitet på kritiske tjenester.

Trådløst nett (WiFi) vil bli driftet av Sykehuspartner, mens innendørs mobilnett vil bli driftet av ekstern leverandør i og utenfor bygget. Denne typen innendørs mobilnett leveranse har grensesnitt i sentrale komponenter som gjør det mulig for andre operatører å koble seg til anlegget.



Ved etablering av en god og fremtidsrettet innendørs mobildekning i byggene brukes HSØs rammeavtale for utbygging av 5G innendørs mobilnett. Leveransen av innendørs mobilnett skal være med i forprosjekt for å sikre nødvendig kartlegging og prosjektering av fiberkabling til bygg, fiberstamnett, samt spredenett-kabling av Cat6a eller bedre for aksesspunkter til mobilnettet.



Figur 15: Logisk topologi for 4G/5G innendørsmobildekning



5G Mid Band 4x4 MIMO + Dual Band 2X2 MIMO			
Max throughput:	2.8 – 3 Gbps	Dimension:	210 mm in diameter
Technology:	GSM, LTE, WCDMA, NR	Weight:	1 500 grams (excluding bracket)
IBW:	100 MHz for mid band; full-band for other bands	Mounting:	One bracket for ceiling or wall mounting
Total Antenna BW:	670 MHz	Color:	Off-white
RF power:	250 mW (TDD) 125 mW (FDD)	Power consumption:	55 W
MIMO:	Single band 4T4R Dual band 2T2R	Operational temp:	+5°C to +40°C (41°F to 104°F)
Antennas:	8 built in omni-directional		

Figur 16: Spesifikasjon av typisk aksesspunkt for 5G mobilnett

<b>Utstyr – Telenor</b>	<b>Dimensjon (mm) (H x W x D)</b>	<b>Vekt (kg)</b>	<b>Maks Effekt</b>	<b>Strømforsyning</b>
Base band Unit (BBU)	44 x 483 x 352 (1U)	9	250 W	48VDC
Transmission CSR	66 x 480 x 364 (1,5U)	7	150 W	48VDC
Indoor Connect IC8855	66 x 441 x 364 (1,5U)	8	100 W	48VDC
Likeretter Eltek FP2 SPS 48VDC	1800 x 600 x 600			
Indoor Radio Unit (IRU)	65 x 487 x 428 (1,5U)		1033W (maks)	230VAC og 48VDC
Likeretter Eltek 48VDC	2U	7		230VAC

Tabell 4: Spesifikasjon for utstyr som inngår i løsningen

## 10 Wifi gjestenett

For pasienter og gjester er det etablert et regionalt IPVPN i kjernenettet for å tilby kontrollert internett-tilgang. Det er dermed adskilt fra alle andre interne nett, og eneste vei ut fra nettet går via en sentral gjestenett-brannmur i det regionale WAN-mottaket. Nettet er felles for både trådløse og trådbundne klienter.

Det er etablert en egen, åpen SSID som heter «SykehusGjest» «HSO Gjest» etter omlegging til nye Cisco c9800 WLC. Ved oppkobling får man tildelt en IP-adresse, og klienten vil begynne å sende trafikk. På den trådløse kontrolleren er det en aksessliste som hindrer gjesteklienter å «snakke» med hverandre.

Gjestenettets kapasitet er i hovedsak begrenset av den tilgjengelige kapasiteten på aksesspunktet man til enhver tid er koblet til, men for å hindre at aktive gjestebrukere skal ta kapasitet fra interne brukere og tjenester brukes QoS «i luften» til å nedprioritere gjesttrafikk etter produksjonstrafikk. Kapasiteten på forbindelsen ut til internett er 2 x 10Gbps, 10Gbps fra hvert datasenter.

I Sykehuspartners sentrale gjestenettbrannmur er det mulig å lage et mer tilpasset regelsett som begrenser tilganger etter HFIenes egne ønsker. Dette vurderes som en endring på et senere tidspunkt.

## 11 Nettverksadministrasjon, overvåkning og logging

Soner for overvåkning og drift av nettverksenheter følger «NO-50 Sikkerhetspolicy for funksjonsdomene kontroll- og administrasjonsplan». For Helseforetakenes lokasjoner er dette segmentert i separate transportnett med tilhørende sone for hvert Helseforetak. Tilsvarende er det for sentrale datasentre og ekstern aksess etablert separate transportnett for drift og overvåkning. Disse nettverkene er tilknyttet Sykehuspartner Sikker Sone.

Transportnettet brukes også for realisering av underliggende nettverk som benyttes av SDA Fabric på Helseforetakenes lokasjoner og ACI Fabric på datasentrene.

### 11.1 Nettverksadministrasjon

Nettverkets administrasjonsgrensesnitt beskyttet ved bruk av Sykehuspartners sonemodell. Dette betyr at helseforetakenes og datasentrenes administrasjonsgrensesnitt er adskilt.

Sykehuspartner PAM benyttes for privilegert tilgang til nettverksenheter og kontrollere i løsningen. Tilgang til administrative grensesnitt støtter direkte bruk av PAM autentiseringsproxier og/eller bruk av jumpservere. Tilgang til jumpservere gis gjennom PAM.

Tilganger som tildeles til nettverkets administrative grensesnitt er basert på prinsipp om rollebasert tilgangskontroll. I dette ligger at man har tilstrekkelig granulering av tilganger basert på behov og roller i nettverket.

Tilgang til administrative grensesnitt er kryptert. Kryptering ivaretar beskyttelsen av både innloggingsdata og selve trafikkstrømmen fra sesjonen. Ved bruk av jumpservere er det kun definerte jumpservere som har tilgang til de administrative grensesnittene til nettverket.

Det er etablert sporbarhet i løsningen slik at administrative oppgaver, tildeling av tilganger, bruk av tilganger og automasjon kan spores. Løsningen inneholder verktøy og brukergrensesnitt for å organisere og administrere autorisasjonen og tilgangskontrollen. For privilegert tilgang overføres logg til regionalt loggmottak iht. gjeldende policy.

## 11.2 Overvåking og logging

Nettverkløsningen har logging og overvåking i henhold til «*NO-40 Formål og krav for drifts- og sikkerhetslogger*». Nettverksenheter sender logger både til egne kontrollere og til Sykehuspartners sentrale loggmottak. Nettverkskontrollere og driftsverktøy sender relevante sikkerhets- og driftslogger til Sykehuspartners sentrale loggmottak.

DNA center administrerer og overvåker Nettverkskomponenter med tanke på inventarkontroll, programvare oppgraderinger, konfigurasjonskontroll, topologi, nedetid, hendelser, problemer og feil gjennom logging, agenter og telemetri. Det er etablert en helhetlig standarddefinisjon over hvilke logg- og telemetridata som eksporteres og/eller gjøres tilgjengelig. Loggdata og intelligens fra overvåking av nettverksenheter sendes videre til sentralt loggdatamottak. Definerte alarmer sendes videre til Sykehuspartners operasjonssenter. Loggdata fra verktøy i løsningen sendes til loggservere, samt til lokal lagring.

Løsningen støtter integrasjon av nettverksadministrasjons- og driftsverktøy med eksisterende verktøyportefølje fra Micro Focus for overvåking, Enterprise Service Management. Løsningen støtter også integrasjon for uthenting av data til CMDB.

## 11.3 Sykehuspartner CERT

Det er et generelt krav om at all datatrafikk skal kunne overvåkes og sendes til Sykehuspartners CERT analyseplattform. Der det er formålstjenlig og i dialog med CERT etableres det avtapping i WAN, LAN, sentrale datasenter og lokale datarom.

Optisk tapping foregår passivt, ingen logisk konfigurasjon er nødvendig da signalet speiles på fysisk nivå. Mottaket til CERT må støtte samme optikk som nettverksenhetene benytter.

Kablingstype må hensynas for å tilrettelegge for optisk tapping. Dette medfører ingen reduksjon i båndbredde ettersom signalet speiles fysisk. Ved bundling av kapasitet eller ved redundans må mottaket korrelere optikk.

## Referanser

- Målarkitektur Nettverk v1.0.docx (fisp.no)
- Målbilde HSØ IKT rom v1.0.docx (fisp.no)
- Modernisering av nett - M0 - Løsningsarkitektur v1.0.docx (fisp.no)
- Modernisering av nett - Løsningsdesign M1-1 Orkestrering og automatisering v1.0.docx (fisp.no)
- Modernisering av nett - Løsningsdesign M1.2 Monitorering overvåkning og nettverksdrift\_v1.0.docx (fisp.no)
- Modernisering av nett - Løsningsdesign M2-1 Ekstern aksess (inter HF WAN) v1.11.docx (fisp.no)
- Modernisering av nett - Løsningsdesign M2-2 HF-LAN\_1.2.docx (fisp.no)
- Modernisering av nett - Løsningsdesign M3.2 Migrering HF-LAN og lokalt datasenter v1.0.docx (fisp.no)
- Modernisering av nett - Løsningsdesign M4 Sentralt datasenter\_v1.02.docx (fisp.no)