# Tjenestebeskrivelse SmartFiber

Versjon 1.6.1

GlobalConnect

# Innhold


1. SmartFiber ..... 4
1.1. Introduksjon ..... 4
2. Funksjonalitet ..... 5
2.1. CPE (Kundeplassert utstyr) ..... 5
2.2. Aksessmetoder og -kapasitet ..... 5
2.3. Lokalt nettverk (LAN) ..... 5
2.3.1 Interne nett ..... 5
2.3.2 Gjestenett ..... 5
2.3.3 LAN- og Wi-Fi-adressering ..... 6
2.3.4 Standard oppsett: DHCP og IP adresseplan ..... 6
2.4. Offentlig IPv4 WAN adresse ..... 7
2.5. SmartFiber-portalen ..... 7
3. Tjenester ..... 8
3.1. Internett ..... 8
3.2. Mobil Aksess Failover ..... 8
3.3. WiFi ..... 8
3.4. Sesjonsbasert brannmur ..... 8
3.4.1 Soneinndeling i sesjonsbasert brannmur ..... 9
3.4.2 Subnett for internt nett ..... 9
3.4.3 Subnett for gjestenett ..... 9
3.5. Service Attack Mitigation ..... 10
3.6. Applikasjonsprioritering ..... 10
3.7. Multilokasjons-oppsett og VPN ..... 10
3.8. Utvidet feilretting ..... 11
3.9. SafeSurf ..... 11
4. Tilleggstjenester ..... 12
4.1. Faste offentlige IP-adresser ..... 12
4.2. Port Forwarding (krever "Faste offentlige IP-adresser") ..... 12
4.3. Ekstern IPsec VPN ..... 12
4.4. SmartFiber Premium ..... 13
4.5. Signalforsterkning for Mobil Aksess ..... 13
4.6. Extended Security ..... 14
4.6.1 Applikasjonskontroll ..... 15
4.6.2 URL omdømme og filtrering ..... 16
4.6.3 IP-omdømme og -filtrering ..... 16
4.7. Extended Switching ..... 18

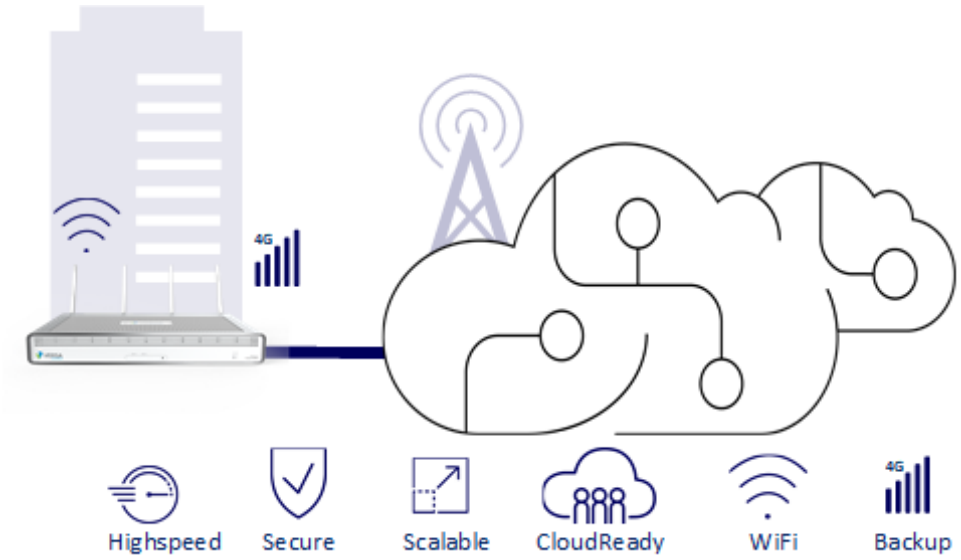
4.8. Extended Wi-Fi ..... 18
4.9. Extended DDoS Protection ..... 19
4.10. ConnectCare ..... 19
5. Geografisk dekning ..... 20
6. Teknisk kvalitet ..... 20
6.1. Grensesnitt for ansvar ..... 20
7. Generelle regler og unntak ..... 20
8. Støttede tilpasninger av SmartFiber ..... 21

# 1. SmartFiber

## 1.1. Introduksjon

SmartFiber er neste generasjons kommunikasjonsløsning, spesielt designet for små og mellomstore bedrifter. Tjenesten leveres som en skytjeneste, noe som forenkler installasjon og drift, fordi alle funksjoner styres sentralt.

- **SmartFiber** driftes av GlobalConnect, som også står for eierskap og drift av CPE (Kundeplassert utstyr) og aksess på kundelokasjonen. GlobalConnect overvåker tilgjengelighet og kvalitet helt til CPE LAN-grensesnittet på kundelokasjonen.




*Figur 1 – SmartFiber konseptet*

SmartFiber inkluderer disse tjenestene:

- Fiber aksess
- Driftet CPE
- WiFi
- Mobil Aksess Failover
- Gjestenett
- Sesjonsbasert brannmur
- Håndtering av nettverksangrep (Service Attack Mitigation)
- Port forwarding / NAT
- Applikasjonsprioritering
- SLA

# 2. Funksjonalitet

## 2.1. CPE (Kundeplassert utstyr)

SmartFiber CPE er den fysiske enheten som er plassert på kundelokasjonen. Denne eies og driftes av GlobalConnect. Enheten har ruter- og brannmurfunksjonalitet.

Tjenesten inkluderer også funksjonalitet for WiFi, og enheten har medfølgende piskantenner som støtter dette formålet.

*Figur 2: SmartFiber CPE (Kundeplassert utstyr)*

## 2.2. Aksessmetoder og -kapasitet

Kundelokasjonen kobles til GlobalConnects infrastruktur med en CPE med to aksesser. Tjenesten leveres med GlobalConnect Internett fiber og en mobil aksess (4G/) for failover. Fiberforbindelsen leveres fra kundelokasjonen til GlobalConnects kjernenettverk via GlobalConnects infrastruktur.

Tjenesten støtter hastigheter opp til 1Gbps på Internett fiber forbindelsen.

## 2.3. Lokalt nettverk (LAN)

SmartFiber tilbyr to lokale subnett som kan benyttes av kunden. Et subnett benyttes av Gjestenettverket for WiFi og LAN-port og et subnett benyttes av Intern nettverket for WiFi og LAN-port.

### 2.3.1 Interne nett

Et WiFi SSID basert nett og et fysisk portbasert nett er samlet som ett subnett for det Interne nettet.

Det fysiske Interne nettet leveres alltid på LAN-port 2. Det Interne nettverket kan kobles sammen på en sikker måte med andre SmartFiber lokasjoner.

### 2.3.2 Gjestenett

Et WiFi SSID basert nett og et fysisk portbasert nett er samlet som ett subnett for gjestenettverk.

Gjestenettverk blir alltid rutet direkte til den lokale Internett tjenesten og kan ikke nås fra andre SmartFiber lokasjoner.

Det fysiske LAN porten til Gjestenetverket leveres alltid på LAN-port 3.

Gjestenetverket er også tilgjengelig som tagged VLAN 20 på Port 2.

### 2.3.3 LAN- og Wi-Fi-adressering

IP adresser og subnett er som standard forhåndsdefinert og basert på private IPv4 adresser (RFC1918). Kunde kan velge å benytte egne RFC1918 subnett på det Interne nettet

| Kunde lokasjon | Subnett Intern nettverk | Subnett Intern WiFi | Subnett Gjeste-nettverk | Subnett Gjeste WiFi |
|---|---|---|---|---|
| Standard oppsett | 10.0.0.0/24 | | 172.16.0.0/24 | |
| Kunde-tilpasset - privat | Kundetilpasset private (RFC1918) IP adresser | | Ikke tilgjengelig for endring | |

Note: Tildelte nettverk skal være "/24", med "255.255.255.0" subnett maske. Hvert subnett inneholder 254 unike adresser.

*Tabell 1: Subnett-plan*

### 2.3.4 Standard oppsett: DHCP og IP adresseplan

| Start adresse | Slutt adresse | Beskrivelse | Subnett |
|---|---|---|---|
| 10.0.0.0 | 10.0.0.9 | Reservert for GlobalConnect | Intern nettverk og Intern WiFi |
| 10.0.0.10 | 10.0.0.20 | Reservert for kundeutstyr med fast IP | Intern nettverk og Intern WiFi |
| 10.0.0.21 | 10.0.0.254 | DHCP tildelt IP adresse | Intern nettverk og Intern WiFi |
| 172.16.0.0 | 172.16.0.9 | Reservert for GlobalConnect | Gjestenettverk og Gjeste WiFi |
| 172.16.0.10 | 172.16.0.20 | Reservert for kunde utstyr med fast IP | Gjestenettverk og Gjeste WiFi |
| 172.16.0.21 | 172.16.0.254 | DHCP tildelt IP adresse | Gjestenettverk og Gjeste WiFi |

*Tabell 2 - Adresseplan*

GlobalConnect benytter følgende DNS-servere: 195.1.0.1 og 195.1.0.2. Tjenesten inkluderer DNS-filter, se avsnitt 3.9 SafeSurf.

Dersom de spesifiserte DNS-serverne slutter å fungere som forventet eller vi ser varig reduksjon i ytelse, kan de bli endret av GlobalConnect.

Dersom det er ønskelig, kan kunde spesifisere DNS-servere ved å kontakte GlobalConnect kundeservice. DNS-serverne kan kun endres for de interne subnettene.

## 2.4. Offentlig IPv4 WAN adresse

Fiberaksessen og mobil aksess Failover har hver sin offentlige IP adresse. Disse adressene kan endres over tid.

Utgående sesjoner fra intern- eller gjestenettet vil benytte disse som kildeadresse ved kommunikasjon mot Internett.

Ved normal drift vil adressen til fiberaksessen benyttes, mens adressen til den mobile aksessen vil benyttes i failover-situasjoner.

Tilleggstjenesten SmartFiber Premium støtter en felles IP adresse for fiberaksessen og mobil aksessen ved hjelp av tuneller, og kan bestilles som en tilleggstjeneste.  Se kapittel 4.4

## 2.5. SmartFiber-portalen

SmartFiber-kunder har tilgang til en egen portal. Her kan kunden blant annet få oversikt over sine tjenester, se tilkoblede enheter, se båndbreddebruk i sanntid, se og endre Wifi-passord og se status på aksesslinjer.

# 3. Tjenester

## 3.1. Internett

Internett-tjenesten som er levert på den underliggende infrastrukturen (fiber eller mobil) brukes for å gi direkte tilgang til Internett fra intern- og gjestenettene. For ytterligere beskrivelse, se Tjenestebeskrivelse Internett.

## 3.2. Mobil Aksess Failover

Med Mobil Aksess Failover vil kundelokasjon kunne fortsette å kommunisere over Internett, selv om en feil skulle oppstå med kjernenettet eller den lokale fiberaksessen.

Dette skjer ved at CPE automatisk bytter til 4G. Trafikk vil bli byttet over til mobil aksessen for fortsatt overføring av data. Failover-tid er opp til 180 sekunder.

Tjenesten inkluderer 100GB data per måned, og er dedikert til det interne subnettet. Trafikk fra gjestenettet vil ikke rutes over failover-forbindelsen.

Det er ikke mulig å kjøpe datapakker for å øke dette volumet.

## 3.3. WiFi

Tjenesten gir tilgang til "On-Box WiFi" på SmartFiber CPE.

CPE er utstyrt med 802.11 a/b/g/n/an/ac (wave2) høy ytelses MIMO dual band (2,4 og 5 Ghz) dual-radio.

For god WiFi-dekning er den anbefalte maksimale romstørrelsen 100 m², med maksimalt 255 samtidige klienter. For best mulig WiFi bør alle klienter ha siktlinje til SmartFiber CPE.

Fysisk plassering av CPE på kundelokasjonen er svært viktig for å sikre gunstig dekning på både WiFi og 4G. Konsulter CPE-installasjonsguiden (medfølger CPE) for retningslinjer. Vi anbefaler dialog med montør når CPE installeres.

WiFi-tjenesten er prekonfigurert med to SSID:

<Firmanavn>-Internal

<Firmanavn>-Guest

Separate passord for hver SSID er prekonfigurert.

Endringer i WiFi-konfigurasjon, som endring av SSID eller passord, utføres ved selvbetjening i Kundeportalen for andre henvendelser bes det kontakte Kundeservice.

Administrative WiFi-konfigurasjoner utføres av GlobalConnect. Hvis Extended WiFi er valgt vil «on-Box WiFi» deaktiveres.

## 3.4. Sesjonsbasert brannmur

CPE har en innebygget, sesjonsbasert brannmur. Denne holder orden på forbindelser mellom WAN (Untrust) og LAN (Intern og Gjest), og sperrer for uautoriserte forsøk på å nå IP adresser på kundens subnet.

Tjenesten inkluderer et predefinert og standardisert regelsett av GlobalConnect, se under

### 3.4.1 Soneinndeling i sesjonsbasert brannmur

Brannmuren er delt inn i 3 ulike sikkerhetssoner.

- Untrust – Internett
- Internal – Subnett for interne adresser, lokale eller på andre lokasjoner
- Guest – Gjestenett

Standard soneoppsett er:

| Til sone -> Fra sone | Untrust | Internal | Guest |
|---|---|---|---|
| **Untrust** | Nekt alle | Nekt alle | Nekt alle |
| **Internal** | Tillat alle | Tillat alle | Nekt alle |
| **Guest** | Tillat alle | Nekt alle | Tillat alle |

*Tabell 3 – Soneinndeling i sesjonsbasert brannmur*

### 3.4.2 Subnett for internt nett

Subnettet for interne nett (se seksjon 2.4.1) blir definert som «Internal» i brannmuren.

Mellom de lokale interne WiFi nettet og fysiske interne LAN port nettet, er det full og ubegrenset tilgang. Sikkerhetssonen «Internal» har tilgang til Internett over levert underliggende infrastruktur.

Dersom kunde har flere lokasjoner vil alle definerte subnett bli lagt inn i denne sonen, slik at alle kundens SmartFiber-lokasjoner er i samme sikkerhetssone.

### 3.4.3 Subnett for gjestenett

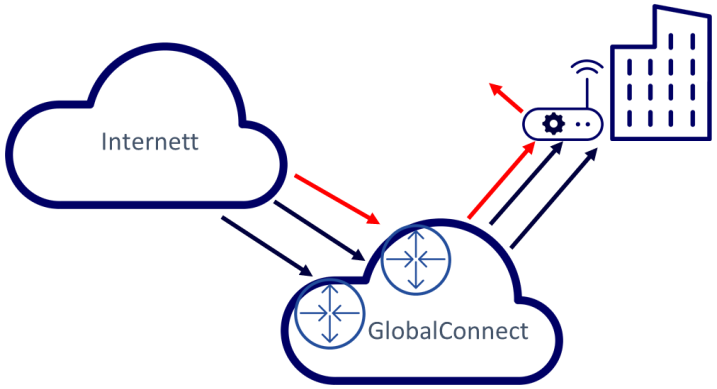
Subnettet for gjestenett (se seksjon 2.3.2) blir definert som «Guest» i brannmuren.

Subnettet for gjestenett har kun tilgang til Internett. Subnettet for gjestenett er isolert fra subnettet for internt nett, og kan ikke nå tjenester eller enheter i disse. Subnettet for gjestenett er også isolert fra andre gjestenett dersom kunde har flere SmartFiber-lokasjoner.

## 3.5. Service Attack Mitigation

Service Attack Mitigation er en funksjon på CPE-en som forhindrer DoS-angrep. Denne typen angrep tar ofte sikte på å overbelaste sesjonstabeller på CPE-en eller andre enheter på nettverket. Service Attack Mitigation benytter mekanismer for beskyttelse mot DoS-angrep (Denial of Service), både mot ressurser på kundes nett og mot SmartFiber CPE.

Service Attack Mitigation begrenser angripers mulighet til å gjennomføre slike tjenestenektangrep ved å begrense trafikkmengden fra den mistenkte kilden til angrepet. Dette gjøres ved analyse av pakkeinformasjon på nettverks- og transportlaget (OSI lag 3 og 4).




## 3.6. Applikasjonsprioritering

For å forhindre at uønsket trafikk skaper overbelastninger eller tregheter i nettet, støtter løsningen prioritering av applikasjoner.

| Profiler | Forretningskritisk trafikk | Annen trafikk | Gjeste trafikk | Type |
|---|---|---|---|---|
| Forretningskritisk | Prioritert | Ingen handling | Strupes | Default |

*Tabell 4: Applikasjons prioriteringsprofil*

Applikasjonene som tilhører " Forretningskritisk", er et fast utvalg bestemt av GlobalConnect.

## 3.7. Multilokasjons-oppsett og VPN

Standard konfigurasjon er uten multilokasjons-oppsett. Dersom en kunde bestiller to eller flere SmartFiber lokasjoner, vil disse kobles sammen i et lukket, kryptert nettverk (VPN).

Alle Multilokasjons SmartFiber settes opp med full-mesh topologi.

Alle lokasjoner i et multilokasjons-oppsett følger en forhåndsdefinert adresseplan. Du kan be om detaljene i denne planen ved å kontakte GlobalConnect kundeservice.

## 3.8. Utvidet feilretting

SmartFiber inkluderer tjenesten Utvidet feilretting. Dette innebærer:

- Reaksjonstid
  - På virkedager fra 07–18 reagerer GlobalConnect på eventuelle feil på tjenesten innen 30 minutter.

- Varsling
  - Kunden varsles om feil på e-post og telefon.

- Håndtering
  - GlobalConnect tar kontakt med kontaktperson hos kunden i løpet av reaksjonstiden for å igangsette feilretting. Dersom feilen ikke løses ved første kontakt, opprettes en sak og informasjon sendes til kunde sentralt.

Utvidet feilretting oppdager feil på tjenesten som innebærer at tjenesten eller 4G er utilgjengelig.

## 3.9. SafeSurf

SafeSurf er en DNS-firewall basert tjeneste som beskytter brukere og systemer fra å komme i kontakt med skadelige nettsteder og/eller bli lurt til å oppgi sensitiv informasjon, for eksempel betalingsinformasjon og passord.

Tjenesten blokkerer tilgang til ondsinnede domener og omdirigerer bruker til en sikker side med varsel om årsak til dette.

GlobalConnect har stort fokus på cybersikkerhet og har valgt å inkludere SafeSurf kostnadsfritt for SmartFiber.

Millioner av nettsider inneholder skadevare i form av Malware/Phishing og vi anbefaler bruk av SafeSurf som et tillegg til andre nødvendige sikkerhetstiltak.

Om man som kunde ikke ønsker å benytte SafeSurf kan man ta kontakt med GlobalConnect kundeservice for å få tjenesten fjernet.

# 4. Tilleggstjenester

## 4.1. Faste offentlige IP-adresser

For kunder som ønsker å gjøre applikasjoner eller tjenester tilgjengelige for Internett fra sitt lokale nettverk, kan kunden velge å få faste WAN IPv4-adresser på fiber forbindelsen.

Den faste IPv4 adressen gjør det også mulig for kunden å bruke alternativene Port forwarding (se avsnitt 4.2) og Extended DDoS Protection Standard (se avsnitt 4.6).

## 4.2. Port Forwarding (krever "Faste offentlige IP-adresser")

Tjenesten støtter port forwarding, også kjent som Inbound NAT (Network Address Translation).

Kunde kan bare bestille Port Forwarding for å gi tilgang til tjenester eller ressurser på det interne subnettet. Port Translation er også mulig.

Port forwarding er bare mulig til statiske IP adresser i det interne subnettet (Eks. Til 10.0.0.10/24).

Port Forwarding/Translation kan settes opp pr. SmartFiber lokasjon i et multilokasjons-oppsett.

Enkelte Application Layer Gateways (ALG) kan benyttes i port forwarding (FTP, TFTP, PPTP, SIP og IKE).

Kunden kan bestille regler for port forwarding (fram til ferdigmelding) eller ved å kontakte kundeservice (etter ferdigmelding).

Fram til ferdigmelding vil de første 10 reglene opprettes kostnadsfritt. Regler utover dette eller alle regler som er bestilt etter ferdigmelding, betraktes som en normal endring og belastes på timebasis.

Visse porter er reserverte for SmartFiber-tjenesten og kan ikke brukes til port forwarding.

## 4.3. Ekstern IPsec VPN

SmarFiber støtter IPSec VPN-tunneler til en ekstern lokasjon.

Ekstern IPSec VPN konfigureres basert på IPSec VPN-standarder og GlobalConnect «Best Practice».

All konfigurasjon og støtte for Ekstern IPSec VPN regnes som en endring (se avsnitt 7.2). GlobalConnect har ingen serviceavtale for Ekstern IPSec VPN.

Som standard bruker IPSec den offentlige IPv4 WAN-adressen som kilde for IPSec-tunnelen og krever derfor Fast WAN IP konfigurert.

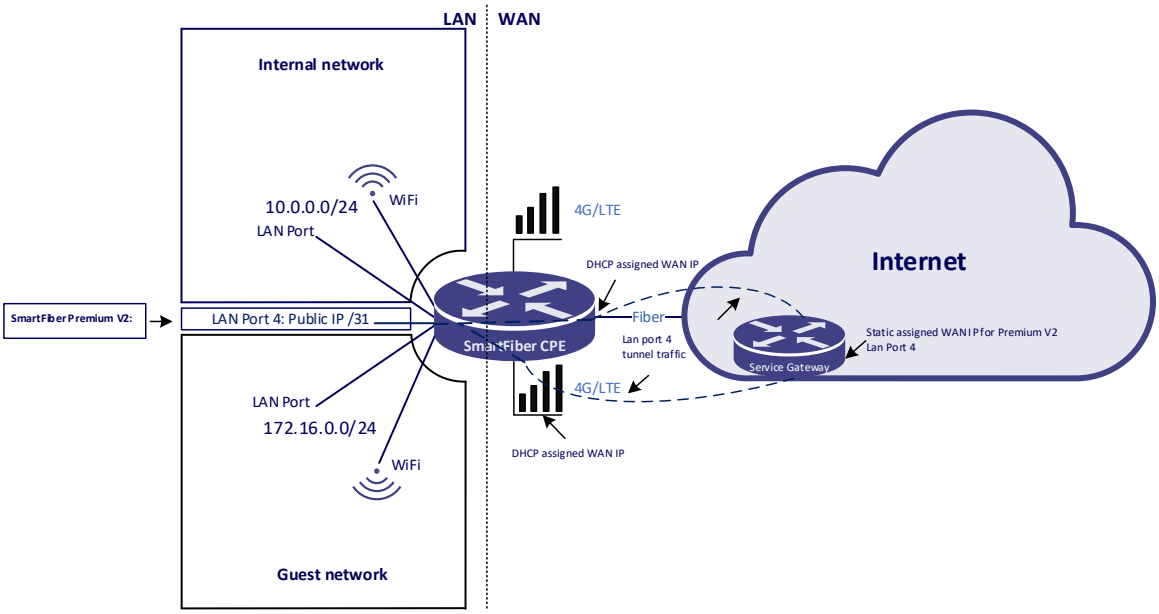
## 4.4. SmartFiber Premium

For kunder som har egen brannmur eller andre enheter som trenger direkte tilgang til offentlig IP-adresser, tilbyr vi SmartFiber Premium.

Premium-alternativet er en fast offentlig IPv4-adresse levert på LAN-port 4 på SmartFiber CPE. Dette prefikset blir ikke filtrert eller analysert av brannmuren i SmartFiber-tjenesten. Standard subnet er /31, 2 stk IP adresser. Adresser opp til /28, 16 stk IP adresser er tilgjengelig som opsjon.

IPv4 adressen vil også være tilgjengelig over 4G failover ved brudd på primær fiber aksess. Trafikken legges automatisk over til 4G, uten endring av din WAN IP adresse, og krever ikke noe tiltak fra kunden. Overgangen mellom primær aksessen og 4G vil kunne ta noen sekunder.

LAN IP adressene tildeles som standard som faste IP adresser. Kunde kan velge å få tildelt LAN IP adressene dynamisk.




*Figur 3: SmartFiber Premium*

## 4.5. Signalforsterkning for Mobil Aksess

Som et tilvalg, kan kunden kjøpe signalforsterkning for mobil aksess. Dette er en kraftigere ekstern antenne for 4G-aksessen med en 5 meter lang kabel og mulighet for utendørs montering. En ytterligere kabel på 10 meter er også inkludert i pakken (maks. 15 meter kabel totalt). Dette er et «gjør det selv»-produkt.

### 4.6. Extended Security

Extended Security tilbyr en Managed Next Generation Firewall (NGFW) basert på en sertifisert programvaredefinert tjeneste, noe som gjør det enkelt og effektivt å installere, endre og administrere.

Extended Security støtter L4-L7 applikasjonsgjenkjenning og beskyttelse mot skadelig programvare, som kan forhindre at filer og programmer lastes ned og kommuniserer med eksterne verter, basert på signaturdatabaser.

Tjenesten gir automatisk oppdatering av objektene for brannmurfunksjonene, inkludert applikasjonskontroll, URL-kategorier og URL / IP omdømme filter.

Extended Security inneholder:

| Produkt | Tjeneste | Beskrivelse |
|---|---|---|
| Extended Security | Applikasjonskontroll | Blokkerer uautorisert internettrafikk basert på applikasjonstype |
| | URL omdømme og filtrering | Unngå uønsket innhold for brukerne og reduser brukereksponering og risiko |
| | IP omdømme og filtrering | Blokker trafikk fra visse IP adresser som er forbundet med dårlig rykte og som kan utgjøre en sikkerhetsrisiko for kundenettverk |
| | Rapportering | Standardrapporter tilgjengelig |

*Tabell 5: «Extended Security» innhold*

Tjenesten inkluderer et forhåndsdefinert regelsett, som er standardisert av GlobalConnect. Kunden kan gjøre opptil 10 regel endringer under installasjonen. En tilpasset regel kan for eksempel være:

- URL omdømme og filtrering: Hvit eller svarteliste URL'er
- IP omdømme og filtrering: Hvit eller svarteliste IP adresser eller subnett

Regler som overstiger dette eller alle regler som er bestilt etter ferdigmelding, betraktes som en konfigurasjonsendring og belastes deretter.

Vi bruker kjente sikkerhetspartnere for å tilby en sikker brannmurtjeneste av høy kvalitet, hver spesialisert innen sitt område:

| Partner | Funksjon |
|---|---|
| Maxmind | GeoIP Database |
| Qosmos | Applikasjon identifisering |
| Webroot | URL og IP Databaser |
| ReversingLabs | Skadelig programvare oppslag/nedlastning |

*Tabell 6: Sikkerhetspartnere*

*Partnerne som brukes kan endres over tid.*

### 4.6.1 Applikasjonskontroll

Applikasjonskontroll tjenesten er utstyrt med applikasjonsgjenkjenning og synlighet. Applikasjonene bestemmes av Deep-Packet-Inspection (DPI) som kjører på alle SmartFiber CPE'er. Dette sikrer at applikasjoner blir gjenkjent så nær kilden som mulig, og at applikasjonsbaserte beslutninger er raske og sikre. Applikasjonsdatabasen for applikasjon inneholder for øyeblikket 3100+ forhåndsdefinerte applikasjoner.

Applikasjonsgjenkjenning er basert på APP-ID, signaturdatabasen bestemmes av Deep Packet Inspection (DPI) ved starten av hver sesjon og etter sesjonshistoriske data.

Hver applikasjon er assosiert med attributter som familie, underfamilie, risiko, produktivitet og koder. Disse kodene kan brukes til å filtrere eller prioritere trafikk.

### 4.6.2 URL omdømme og filtrering

URL filtrering gir kontroll over nettlesingsaktivitet. Det forhindrer brukeren å få tilgang til uproduktive nettsteder eller nettsteder som er forbundet med kriminelle aktiviteter eller har høy sikkerhetsrisiko.

Dette gir forbedret beskyttelse mot sofistikerte trusler, inkludert skadelig programvare og phishing nettsteder.

Filtrering er basert på kategorier og forhåndsdefinerte svart/hvit lister. Inkludert i produktet er profilen “URL-filter-basic”, se tabellen nedenfor. Kunden kan velge en strengere profil, “URL-filter-extended“. Svart/hvit oppføring på URL nivå er tillatt. Dette kan gjøres under installasjonen, eller som en endringsordre etter at tjenesten er levert og prises etter medgått tid.

| Profil | URL kategorier |
|---|---|
| URL-filter-basic (standard) | • bot_nets<br>• Malware_sites<br>• phishing_and_other_frauds<br>• proxy_avoid_and_anonymizers |
| URL-filter-extended | • adult, pornography, hacking and nudity<br>• parked_domains<br>• private IP adresser |

*Tabell 7: URL kategorier*

IP filtreringsprofilen kombinert med URL filtrering kan sammen blokkere dårlig trafikk (IP adresser) og unngå falske positive når IP adresser deles for forskjellige tjenester. Det er veldig vanlig å ha samme IP for forskjellige nettsteder, og med URL filtrering kombinert kan det bidra til å skille de gode IP adressene til URL’er fra de dårlige tjenestene (IP adresser). I dette tilfellet vil trafikken som treffer en URL-filterkategorier bli stoppet. Samtidig vil trafikken som treffer IP filterets omdømme også bli stoppet.

I tilfelle URL trafikk treffer både et URL filter og IP filter, vil en troverdig URL omdømme ha forrang som standard.

Skadelig programvare funksjonen blokkerer tilgang til uønsket nettinnhold for å redusere risikoen og eksponeringen for f.eks. nedlastning av skadelig programvare og phishing-forsøk.

### 4.6.3 IP-omdømme og -filtrering

IP omdømme og filtrering kan brukes til å blokkere trafikk fra visse IP adresser som er assosiert med et dårlig omdømme, IP adresse og dens geografiske beliggenhet, som kan utgjøre en sikkerhetsrisiko for et kundenettverk.

«Extended Security» tjenesten inkluderer en forhåndsdefinert profil beskrevet nedenfor. Kunden kan legge til regler for hvit- eller svart-liste IP-adresser/subnett. Dette kan gjøres under installasjonen, eller som en endringsordre etter at tjenesten er levert og prises etter medgått tid.

| IP filter navn | Handling | Samsvar | IP omdømme inkluderer |
|---|---|---|---|
| Blokker uønsket trafikk | Avvis | Kilde eller destinasjon | **Botnet** avviser kjente verter fra Botnet C & C-kanaler, og infiserte zombie-maskiner kontrollert av Bot master.<br><br>**Skannere** nekter kjente verter fra rekognosering som prober, verts-skanning, domeneskanning og passord brute force angrep.<br><br>**Omdømme** nekter tilgang fra IP adresser som for tiden er kjent for å være infisert med skadelig programvare. Inkluderer også IP'er med gjennom-snittlig lav Webroot Reputation Index score. Aktivering av denne kategorien forhindrer tilgang fra kilder som er identifisert for å kontakte distribusjons-steder for skadelig programvare.<br><br>**Windows Exploits** nekter aktive IP adresser som tilbyr eller distribuerer skadelig programvare, shell kode, rootkits eller ormer.<br><br>**Web Attacks** nekter kjente verter fra å utføre skripter på tvers av nettsteder, iFrame injeksjon, SQL injeksjon, injeksjon på tvers av domener eller brute force-angrep på domenepassord.<br><br>**Spam Sources** nekter tunnelering av spam meldinger gjennom en proxy, anonyme SMTP aktiviteter og forum spam aktiviteter.<br><br>**Phishing** nekter IP-adresser som er vert for phishing-nettsteder og andre typer svindel-aktiviteter som annonseklikksvindel eller spillsvindel.<br><br>**Proxy** nekter IP-adresser som gir proxy-tjenester. |

*Tabell 8: IP omdømme og filtrering*

Skadelig programvare-funksjonen blokkerer kommunikasjon med uønskede webtjenester for å redusere risikoen og eksponeringen for f.eks. botnets, exploits, proxies.

## 4.7. Extended Switching

Extended Switching er en tilleggstjeneste til SmartFiber. Tjenesten lar kunden bruke de tilgjengelige LAN-portene på SmartFiber CPE-en som en lag 2 nettverksswitch. Tjenesten baserer seg på Layer 2 Forwarding-teknologien.

Tjenesten er prekonfigurert etter følgende oppsett.

| Default IRB details | Network Name | VLAN id | Zones | Routing Instances | Network |
|---|---|---|---|---|---|
| L3 interface details | internal | 1 | internal | internal | 10.0.0.0/24* |
| | guest | 20 | guest | guest | 172.16.0.0/24 |

*IP-adressene kan endres på forespørsel.

| Default Switch details | Port/antenna | VLAN | Switch mode | Native VLAN |
|---|---|---|---|---|
| L2 interface details | Port 2 | Internal | Access | Internal |
| | | Guest | Trunk | |
| | Port 3 | Guest | Access | |
| | Port 4* | Internal | Access | |
| | Port 6 | Internal | Access | |
| | Port 7 | Internal | Access | |
| | Port 8 | Internal | Access | ‘ |
| | Port 9 | Internal | Access | |
| | Wi-Fi | Internal | Access | |
| | | Guest | Access | |

*Port 4 er ikke tilgjengelig for Extended Switching hvis kunden har SmartFiber Premium.

## 4.8. Extended Wi-Fi

Extended Wi-Fi er en tilleggstjeneste til SmartFiber. Tjenesten tilbyr bransjeledende teknologi og maskinvare, en svitsj, og trådløst lokalt nettverk som en administrert tjeneste.

Tjenesten inkluderer installasjon, drift, vedlikehold og overvåking av utstyret i kundens lokaler og kan kjøpes i to forskjellige pakker:

**Standard**

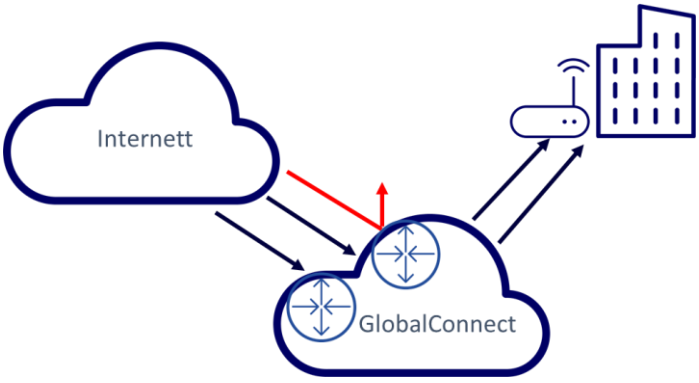
- Intern 4 port PoE svitsj i SmartFiber ruteren
- 1 stk. AP, aksess punkt
- Støtter maks 3 aksess punkter

**Pluss**

- Ekstern PoE svitsj
- 2 stk. AP, aksess punkter
- Støtter maks 5 aksesspunkter

For ytterligere informasjon om tjenesten, se spesifikk Tjenestebeskrivelse for Extended WiFi.

## 4.9. Extended DDoS Protection




Extended DDoS Protection Standard er en tilleggstjeneste til SmartFiber, som tilbyr mer utstrakt beskyttelse mot DDoS-angrep enn det som tilbys som standard i SmartFiber (Service Attack Mitigation). Extended DDoS Protection Standard beskytter kjernenettet og kunde aksessen. Den baserer seg på filtreringspunkter i GlobalConnects kjernenett som analyserer metadata på lag 3 og 4 i trafikken. Ved identifisering av kjente trusler basert på informasjon i disse lagene, iverksettes automatisk filtreringsregler som beskytter kundens nettverk.

Trafikken analyseres ved hjelp av stikkprøver. Det vil være en liten forsinkelse fra et angrep oppdages til filtreringsreglene iverksettes, og ved flere etterfølgende angrep kan det oppstå korte avbrytelser i sammenheng med dette; men lange avbrytelser i forbindelsen skal ikke skje.

Typisk tar et DDoS-angrep-sikte på å overbelaste aksessen mellom tjenesteleverandør (GlobalConnect) og kunde med unormalt høy trafikk volum. Ved å gjøre filtreringen i GlobalConnects kjernenett istedenfor på CPE-en, unngår kunden at aksessen, samt CPE-en, kan overbelastes av DDoS-angrep.

Extended DDoS Protection Standard krever Faste offentlige IP-adresser.

## 4.10. ConnectCare

ConnectCare er utviklet for å gi kunden ekstra forutsigbarhet, fleksibilitet og motstandsdyktighet mot svingninger i markedet. ConnectCare er kun tilgjengelig ved avtaleperiode på minst 36 måneder.

Med ConnectCare får kunden:

- Forutsigbarhet:
  - GlobalConnect garanterer null prisjusteringer (indeksjusteringer) gjennom kontraktsperioden.
- Fleksibilitet:
  - Kunden kan flytte sitt SmartFiber-abonnement uten ekstra kostnad til en adresse hvor GlobalConnect har egen infrastruktur, én gang ila. kontraktsperioden, etter minimum seks måneder fra tjenesten er levert.
- Motstandsdyktighet:
  - Kunden kan fryse sitt SmartFiber-abonnement i opptil tre måneder (én, to eller tre hele måneder), én gang i løpet av kontraktsperioden, etter minimum seks måneder. I disse månedene faktureres det kun for Connect Care. Frys gjelder fra første påfølgende faktureringsperiode etter aktivering. Tjenesten er ikke tilgjengelig i frys perioden.

# 5. Geografisk dekning

SmartFiber er tilgjengelig i Norge og Danmark.

# 6. Teknisk kvalitet

SmartFiber følger spesifikasjonene for underliggende infrastruktur med tanke på SLA, garanti og responstid. Tjenestekvalitet for SmartFiber defineres i separat Tjenestekvalitets dokument og inkluderer Servicetid Utvidet med Servicegaranti 2.

Det kan være lokale variasjoner i forskjellige land.

## 6.1. Grensesnitt for ansvar

Grensesnittet mellom kunden og GlobalConnect er ruterens LAN-grensesnitt.

GlobalConnect er ansvarlig for levering og drift av tjenesten og ruter. Kunden er ansvarlig for lokalt nettverk og internkabling på hvert sted.

Når den innledende installasjonen er gjennomført og kunden begynner å ta tjenesten i bruk, kan det være nødvendig å starte om eller rekonfigurere utstyr som er tilkoblet nett (for eksempel servere, datamaskiner, skrivere, Smart-TV, og nettverkstilkoblede lydenheter). GlobalConnect tar ikke ansvar for enheter på kundens lokalnett.

# 7. Generelle regler og unntak

- Etter bestilling og fram til ferdigmelding av leveransen, vil alle endringer kunden ønsker innenfor spesifiserte støttede tilpasninger gjennomføres uten ekstra kostnad.
- Etter at leveransen er ferdigmeldt vil ønskede endringer innenfor spesifiserte støttede tilpasninger faktureres i henhold til gjeldende prisliste
- FastTrack er ikke tilgjengelig for SmartFiber Premium
- Det er bare den offentlige IP-adressen på fiberaksessen som kan benyttes for port forwarding og det er ikke mulig å benytte port forwarding dersom fiberaksessen ikke er aktiv (på Mobil Aksess Failover).
- Det er ikke mulig å benytte gjestenettet for tilgang til Internett (se seksjon 3.1) dersom fiberaksessen ikke er aktiv (på Mobil Aksess Failover).
- Utenfor Norge kan internkabling i bygninger eies av GlobalConnect eller en av GlobalConnects underleverandører.
- Det er ingen garanti for sambandskvalitet eller båndbredde på Mobil Aksess Failover.
- CPE kan ikke flyttes fra installasjonsadressen som er spesifisert i kontrakten uten skriftlig samtykke fra GlobalConnect
- SIM-kortet er en integrert del av CPE. Det er GlobalConnects eiendom, og det er ikke tillatt å fjerne eller bytte ut kortet.
- SmartFiber-portalen er pt. kun tilgjengelig i Norge.

## 8. Støttede tilpasninger av SmartFiber

Endringer støttet av kundeservice og fakturert på timebasis.

- Endring av WiFi SSID for både gjestenett og internt nett.
- Endring av WiFi passord for både gjestenett og internt nett.
- Deaktivering av «On-box WiFi» (Begge SSID).
- Endring av DNS servere in DHCP-tjenesten (kun for interne subnett).
- Oppsett og endring av Port Forwarding.
- Endring av LAN IP RFC1918 adresse subnett for Internal
- Endring av SmartFiber Premium LAN IP-adresse tildeling. Fast eller dynamisk.
- Utsendelse av komplett IP-plan for SmartFiber multilokasjoner.
- Endre/legge til regler i Extended Security
    - URL omdømme og filtrering: Svart/hvit liste URL'er
    - URL omdømme og filtrering: Bytte mellom «Basic» eller «Extended» profil
    - IP omdømme og filtrering: Svart/hvit liste IP adresser eller subnett
    - Applikasjonskontroll: Svart/hvit liste spesifikke applikasjoner. Støtter bare kjente applikasjoner.
    - Extended Security: Deaktivere rapport via e-post.

Endringer som må håndteres av salgsrepresentanten og medfører en MRC eller endring av abonnement/abonnementsavgift.

- Legge til/fjerne Fast offentlig WAN IPv4 tilleggstjeneste.
- Legge til/fjerne SmartFiber Premium tilleggstjeneste
- Legge til/fjerne «Extended Security»
- Legge til/fjerne «Extended WiFi»
- Endre SmartFiber lokasjoner fra «Stand Alone» til «Multi-lokasjon»-modus. Obs: Krever full re-installasjon av hele tjenesten