Tjenestebeskrivelse SmartFiber

Versjon 1.3.2

GlobalConnect

GlobalConnect

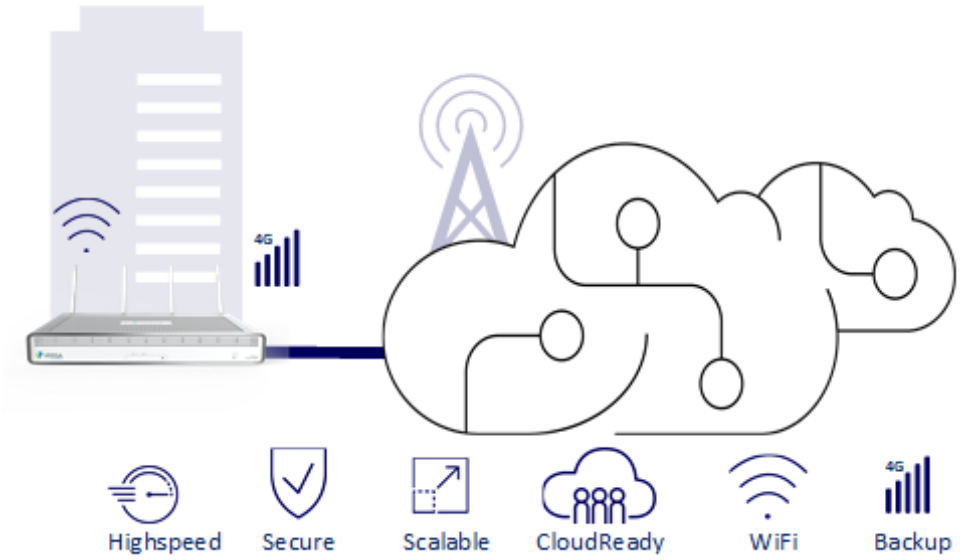
Innhold

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
- Wi-Fi
- 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 Wi-Fi, 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/LTE) for failover.

Fiberforbindelsen leveres fra kundelokasjonen til GlobalConnects kjernenettverk via GlobalConnects egen infrastruktur.

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

2.3. LAN porter

SmartFiber tilbyr fire lokale subnett som kan benyttes av kunden. To av nettene er levert som Wi-Fi (2 x SSID), og to som fysiske LAN-porter.

2.3.1 Internt nett

Et Wi-Fi SSID basert subnett og et fysisk portbasert subnett er samlet som ett Internt nettverk.

Dermed består det interne nettverket av to subnett. En tilknyttet Wi-Fi SSID og den andre tilknyttet den fysiske LAN porten.

Interne nettverk kan kobles sammen på en sikker måte med andre SmartFiber lokasjoner.

2.3.2 Gjestenett

Et Wi-Fi SSID basert subnett og et fysisk portbasert subnett er samlet som ett gjestenettverk.

Dermed består gjestenettverket av to subnett. En tilknyttet Wi-Fi SSID og den andre tilknyttet den fysiske LAN- porten.

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

2.4. LAN og WiFi adressering

IP adresser og subnett er forhåndsdefinert og basert på private IPv4 adresser (RFC1918):

Lokasjon	Subnett Intern nettverk	Subnett Intern Wi-Fi	Subnett Gjeste-nettverk	Subnett Gjeste Wi-Fi
Kunde lokasjon	10.0.0.0/24	10.0.8.0/24	172.16.0.0/24	172.16.8.0/24

Note: Alle nettverk er "/24", altså med "255.255.255.0" subnett maske. Hvert subnett inneholder 254 unike adresser.

Tabell 1: Subnett plan

2.4.1 DHCP og IP adresseplan

Start adresse	Slutt adresse	Beskrivelse	Subnett
10.0.0.0	10.0.0.9	Reservert for GlobalConnect	Intern nettverk
10.0.0.10	10.0.0.50	Reservert for kundeutstyr med fast IP	Intern nettverk
10.0.0.51	10.0.0.250	DHCP tildelt IP adresse	Intern nettverk
10.254.254.10	10.254.254.250	Reservert for ClientVPN	Intern VPN
10.0.8.0	10.0.8.9	Reservert for GlobalConnect	Intern Wi-Fi
10.0.8.10	10.0.8.50	Reservert for kundeutstyr med fast IP	Intern Wi-Fi
10.0.8.51	10.0.8.250	DHCP tildelt IP adresse	Intern Wi-Fi
172.16.0.0	172.16.0.9	Reservert for GlobalConnect	Gjestenettverk
172.16.0.10	172.16.0.50	Reservert for kunde utstyr med fast IP	Gjestenettverk

Start adresse	Slutt adresse	Beskrivelse	Subnett
172.16.0.51	172.16.0.250	DHCP tildelt IP adresse	Gjestenettverk
172.16.8.0	172.16.8.9	Reservert for GlobalConnect	Gjeste Wi-Fi
172.16.8.10	172.16.8.50	Reservert for kunde utstyr med fast IP	Gjeste Wi-Fi
172.16.8.51	172.16.8.250	DHCP tildelt IP adresse	Gjeste Wi-Fi

Tabell 2 - Adresseplan

GlobalConnect benytter følgende DNS-servere: 8.8.8.8 og 8.8.4.4

Vær oppmerksom på at GlobalConnect ikke drifter denne tjenesten, og at vi derfor ikke kan gjennomføre feilsøking og -retting på denne. 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.

2.5. 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 den fiberaksessen benyttes, mens adressen til den mobile aksessen vil benyttes i failover-situasjoner.

Den offentlige IP adressen på fiberaksessen og mobil aksess er ikke den samme.

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.

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/LTE. 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 Wi-Fi" på SmartFiber CPE.

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

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

Fysisk plassering av CPE på kundelokasjonen er svært viktig for å sikre optimal dekning på både Wi-Fi og 4G/LTE. Konsulter CPE-installasjonsguiden (medfølger CPE) for retningslinjer.

Wi-Fi-tjenesten er prekonfigurert med to SSID:

<Firmanavn>-Internal

<Firmanavn>-Guest

Separate passord for hver SSID er prekonfigurert.

Endringer i Wi-Fi konfigurasjon utføres av GlobalConnect ved henvendelse til Kundeservice, som f.eks. ending av SSID eller passord, eller avstenging av "On-Box Wi-Fi" (deaktiverer SSID for både intern- og gjestenettet).

Administrative Wi-Fi-konfigurasjoner utføres av GlobalConnect.

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

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

Mellom de lokale interne subnettene 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

Subnettene for gjestenett (se seksjon 2.4.2) blir definert som «Guest» i brannmuren.

Det er ingen begrensninger i tilgangen mellom disse.

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

3.5. Service Attack Mitigation

Tjenesten benytter mekanismer for beskyttelse mot DoS (Denial of Service) for å håndtere angrep, både mot ressurser på kundes nett og mot SmartFiber CPE.

Service Attack Mitigation eller håndtering av nettverksangrep, begrenser angripers mulighet til å gjennomføre kvantitetsbaserte 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

Dersom en kunde bestiller to eller flere SmartFiber lokasjoner, vil disse som standard kobles sammen i et lukket, kryptert nettverk (VPN).

Alle SmartFiber-lokasjoner 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.

Hvis kunden ikke ønsker å ha to eller flere lokasjoner sammenkoblet, kan en lokasjon merkes som "Stand Alone" som vil deaktivere all kommunikasjon med andre lokasjoner for den lokasjonen.

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 alternativet Port forwarding (se avsnitt 4.2).

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 fysiske LAN port subnettet. Port Translation er også mulig.

Port forwarding er bare mulig til statiske IP adresser i det interne fysiske LAN port 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).

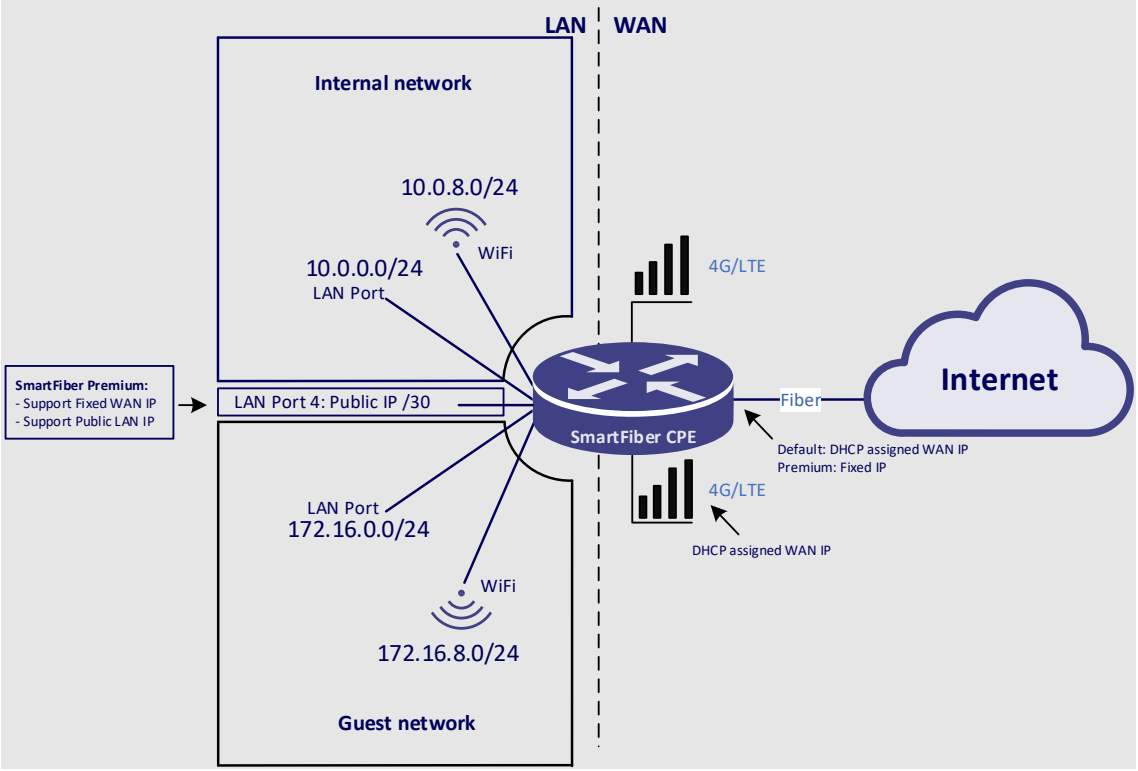
Fram til ferdigmelding vil de første 10 reglene opprettes kostnadsfritt. Regler utover dette eller alle regler som er bestilt etter ferdigmelding, betraktes som en normal endring og belastes på timebasis.

4.3. SmartFiber Premium (krever "Faste offentlige IP-adresser")

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

Som standard gis det en offentlig IP adresse for kunden. Kunden kan velge opp til et /28 offentlig subnett. Kunden kan be om et større subnett under installasjonen eller ved å kontakte kundeservice etter ferdigmelding. Vær oppmerksom på at et større subnett medfører tilleggskostnader basert på gjeldende IP adresse priser.

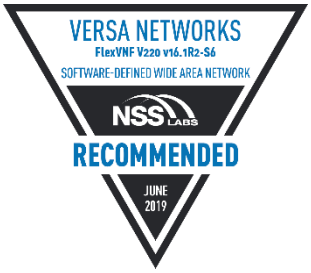
Premium alternativet er en fast offentlig IPv4 adresse levert på LAN port på SmartFiber CPE. Dette prefikset blir ikke filtrert eller analysert av brannmuren i SmartFiber tjenesten.



Figur 3: SmartFiber Premium

SmartFiber Premium krever “Faste offentlige IP-adresser” tilvalget.

4.4. 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.

Tjenesten er en tilleggstjeneste til SmartFiber, derfor er SmartFiber en forutsetning for å kjøpe Extended Security tjeneste.

Extended Security støtter L4-L7 applikasjons gjenkjenning og beskyttelse mot skadelig programvare, som forhindrer at filer og programmer lastes ned og kommuniserer med ekstern host basert på signaturdatabaser.

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

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.

4.4.1 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.

4.4.2 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 • Malware_sites

Profil	URL kategorier
	• phishing_and_other_frauds • proxy_avoid_and_anonymizers
URL-filter-extended	• adult, pornography, hacking and nudity • parked_domains • 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 et **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.

4.4.3 Rapportering og logging

«Extended Security» tjeneste inkluderer synlighet og analyse av trafikken. Informasjonsvisningen for analyse er basert på trafikklogger som sendes kunde pr. e-post månedlig.

Tjenesten inkluderer en flerdimensjonal sikkerhetsrapport:

- NGFW - topp applikasjoner/URL/ protokoller/regler/src og dst ip
- Applikasjonsstatestikk - regellogger basert på stoppet applikasjoner
- URL filtrering - topp URL-kategorier/omdømme/kilde osv.
- Logger - tilgang/IP filtrering /URL-filtrering /DoS etc.

Logging er aktivert for følgende funksjoner; Applikasjons blokkeringsregler, URL filtrering, IP filtrering. Funksjonen er tilgjengelig for GlobalConnect kundeservice og benyttes i feilrettings prosessen.

4.4.4 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. **Skannere** nekter kjente verter fra rekognosering som prober, vertsskanning, domeneskanning og passord brute force angrep. **Service Attach Mitigation** forhindrer DOS-angrep (DOS), unormal synkroniseringsflom og unormal trafikkdeteksjon på CPE. **Omdømme** nekter tilgang fra IP adresser som for tiden er kjent for å være infisert med skadelig programvare. Inkluderer også IP'er med gjennomsnittlig lav Webroot Reputation Index score. Aktivering av denne kategorien forhindrer tilgang fra kilder som er identifisert for å kontakte distribusjonssteder for skadelig programvare. **Windows Exploits** nekter aktive IP adresser som tilbyr eller distribuerer skadelig programvare, shell kode, rootkits eller ormer. **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. **Spam Sources** nekter tunnelering av spam meldinger gjennom en proxy, anonyme SMTP aktiviteter og forum spam aktiviteter.

IP filter navn	Handling	Samsvar	IP omdømme inkluderer
			Phishing nekter IP-adresser som er vert for phishing-nettsteder og andre typer svindelaktiviteter som annonseklikksvindel eller spillsvindel. **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.

4.4.5 Extended Remote Work

SmartFiber støtter Extended Remote Work, som er en klient VPN tjeneste.

Tilleggstjenesten Extended Remote Work gjør det mulig for eksterne brukere å koble seg sikkert til SmartFiber nettverket.

En programvare er installert på kundens bærbare datamaskiner og datamaskiner som krever ekstern tilgang. Ved å bruke applikasjonen og SmartFiber Extended Remote Work tjenesten, kan brukere på reise eller brukere som jobber hjemmefra, få tilgang til ressurser på kundens SmartFiber lokasjon. F.eks. applikasjoner, filer og skrivere.

Når en bruker hos kunden aktiverer applikasjonen, fremmes en forespørsel om brukernavn og passord. Hvis brukeren blir autentisert, vil brukeren være koblet til kundens SmartFiber interne nettverk ved hjelp av den sikre og krypterte Extended Remote Work tjenesten.

Extended Remote Work tilbyr:

- Klient: Windows 10 eller MacOS
- AD integrasjon. Microsoft LDAP-autentisering
- Opptil 100 eksterne brukere (trinn 10, 50 og 100)
- Mulighet for split tunnel (deaktivert som standard)

Brukere blir autentisert av kundens AD tjeneste som tilbys av kunden. Autentiseringslenken mellom tjenesten Extended Remote Work og kundens AD etableres under implementeringsprosessen.

Extended Remote Work bruker AES256 eller tilsvarende som krypteringsmetode.

Split Tunnel alternativet gir brukerens bærbare PC/PC muligheten til å laste internett-trafikk direkte i stedet for å transportere den til SmartFiber lokasjonen. Dette kan gi eksterne brukeren bedre ytelse, spesielt om brukeren er koblet på over store avstander. Sikkerhetsnivået kan imidlertid bli noe redusert, siden ikke all trafikk inspiseres av SmartFiber brannmuren.

Brukerne får de samme DNS-serverne som “Internt nettverk” DHCP. IP adresser er fra IP planen som er beskrevet i avsnitt 2.4.1.

5. Geografisk dekning

GlobalConnect tilbyr tjenesten i Norge, Sverige og Danmark, og er forbeholdt lokasjoner der GlobalConnect har egen fiber.

6. Teknisk kvalitet

SmartFiber følger spesifikasjonene for underliggende infrastruktur med tanke på SLA, garanti og responstid. 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.

Som en del av vårt SmartFiber-produkt kan vi tilby en tilleggstjeneste, en «kom-på-nett garanti», som innebærer at en av våre sertifiserte partnere bistår kunden, på kundens lokasjon, med nødvendige konfigurasjonsendringer. Ta kontakt med din salgsrepresentant eller GlobalConnect kundeservice for pristilbud.

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
- Fast offentlig IP for Mobil Aksess Failover kan kun leveres i Danmark
- SmartFiber Premium-tilvalget støtter ikke Mobil Aksess Failover. Den faste offentlige IP-adressen på LAN porten kan kun benyttes gjennom fiberaksessen.
- 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 dersom fiberaksessen ikke er aktiv (på Mobil Aksess Failover).
- «Kom-på-nett garanti» leveres kun i Norge
- 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.

8. Støttede tilpasninger av SmartFiber

Endringer støttet av kundeservice og fakturert på timebasis.

- Endring av Wi-Fi SSID for både gjestenett og internt nett.
- Endring av Wi-Fi passord for både gjestenett og internt nett.
- Deaktivering av «On-box Wi-Fi» (Begge SSID).
- Endring av DNS servere in DHCP-tjenesten (kun for interne subnett).
- Sette SmartFiber lokasjoner i «Stand Alone»-modus.
- Oppsett og endring av Port Forwarding.
- 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 Remote Work: Aktivere/deaktivere split-tunnel alternativet

- Extended Security: Deaktivere rapport via e-post.

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

- Legge til/fjerne fast IPv4 offentlig tilleggstjeneste. Maks /28 subnett kan legges til.
- Legge til/fjerne SmartFiber Premium tilleggstjeneste
- Legge til/fjerne «Extended Security»
- Extended Remote Work: Legge til, fjerne eller endre mellom brukernivåer