Tjenestebeskrivelse IP-VPN

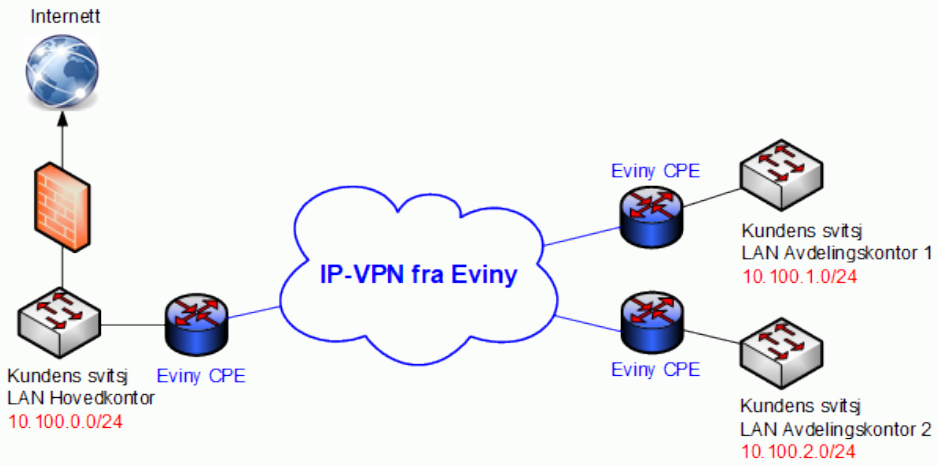
eviny

Innhold

Evinys IP-VPN tjenester

Bedriftsnett IP-VPN fra Eviny er en sikker og robust løsning for kommunikasjon mellom to eller flere lokasjoner. Bedriftsnett IP-VPN blir bygget på Evinys MPLS infrastruktur. Dette gir Eviny mulighet til å levere en stabil tjeneste med høy oppetid og god kvalitet. Ved ønske om tilknytning i IP-VPNet i et område der Eviny ikke har egen infrastruktur, kan Eviny levere sambandet gjennom en av våre samarbeidspartnere, og vi kan således levere Bedriftsnett IP-VPN med aksesser over hele landet.

I et Bedriftsnett IP-VPN er all trafikk 100% adskilt fra andre kunders trafikk, og IP-VPN benyttes av bedrifter og institusjoner med høye krav til sikkerhet.



Skissen over viser et eksempel på Bedriftsnett IP-VPN fra Eviny. Rent logisk ser et IP-VPN for kunden ut som en rutet tjeneste som knytter sammen to eller flere LAN fra ulike lokasjoner. Vanligvis har hovedkontoret en internettlinje som også avdelingskontorene benytter gjennom IP-VPNet. Bedriftsnett IP-VPN er svært skalérbart, og det er ingen praktisk øvre grense for hvor mange lokasjoner som kan tilknyttes IP-VPNet. Konfigurasjon av IP-VPNet utføres av Eviny i henhold til spesifikasjonene gitt fra kunde. Eviny kan bistå kunden med design av IP-VPNet.

IP-VPN Managed

IP-VPN fra Eviny kan leveres med kunderuter (CPE) på hver lokasjon. For kunden betyr dette en nøkkelferdig løsning, der Eviny står for all konfigurasjon og drift av ruting i IP-VPNet – Kunden trenger bare å koble til sin LAN-svitsj på hver lokasjon.

Med CPE fra Eviny, har Eviny god kontroll over tjenesten som blir levert, med rask og effektiv feilsøking ved evt problemer, samt mulighet for tilleggsprodukter som QoS, flere tjenestenett, overvåking og rapportering. Det tas automatisk backup av konfigurasjon på kunderuterne. Eviny benytter kvalitetsprodukter fra Cisco.

Kunden kan få SNMP lesetilgang til kunderuterne i sitt IP-VPN, og har anledning til å hente trafikkdata og annen informasjon inn i kundens egne overvåking- og managementsystemer.

IP-VPN Unmanaged

Med IP-VPN Unmanaged administrerer og drifter kunden sine egne CPEer i IP-VPNet. Kunden har dermed full kontroll over utstyrsvalg, funksjonalitet, konfigurasjon, overvåking, feilsøking og sikkerhet på alle lokasjoner.

Eviny anbefaler at det konfigureres dynamisk ruting med BGP mellom CPEer og IP-VPNet. På denne måten får kunden en standardisert og fleksibel tjeneste, og kan etablere og endre LAN-adressering i nettverket etter behov, uten å måtte involvere Eviny.

IP-adresser

Bedriftsnett IP-VPN er en rutet lag3-tjeneste, og det må derfor etableres egne subnett på hver lokasjon. Kunden er ansvarlig for tildeling av LAN-adresser på alle lokasjoner. Eviny konfigurerer disse LAN-adressene på kunderuterne og sørger for ruting mot LAN-adressene i IP-VPNet.

Eviny kan levere IP-VPN med dual-stack IPv4 og IPv6. Kunden administrerer hvilke IPv6 LAN-adresser som skal benyttes på hver lokasjon, ut fra IPv6-adressene som kunden har fått tildelt fra sin internettleverandør, enten det er Eviny eller en annen leverandør.

MTU

IP-VPN fra Eviny leveres med MTU (standard pakkestørrelse) på 1500 byte. Ved behov kan MTU økes.

Dynamisk ruting

Hvis kunden ønsker dynamisk ruting i IP-VPNet og mellom Evinys kunderuter og kundens eget utstyr, kan dette konfigureres. Eviny kan da konfigurere BGP eller OSPF mot kundens utstyr.

Grensesnitt

Standard grensesnitt for tilkobling av sluttbrukers utstyr er RJ45 med GigabitEthernet 10/100/1000Base-TX. Sammenkobling gjøres med TP (Twisted Pair) kabel.

Det anbefales å benytte Auto hastighet og Auto dupleks.

Ved behov kan det avtales fiberoptisk grensesnitt 1000Base-SX/LX. Hvis det benyttes fiberoptisk grensesnitt er det vanlig med singelmodus fibermoduler i endeutstyret og fiberkonnektorer av typen SC eller LC. Det vil spesifiseres ved leveranse hvilken konnektor type som benyttes. Kunde må ha tilsvarende fibermodul i eget utstyr.

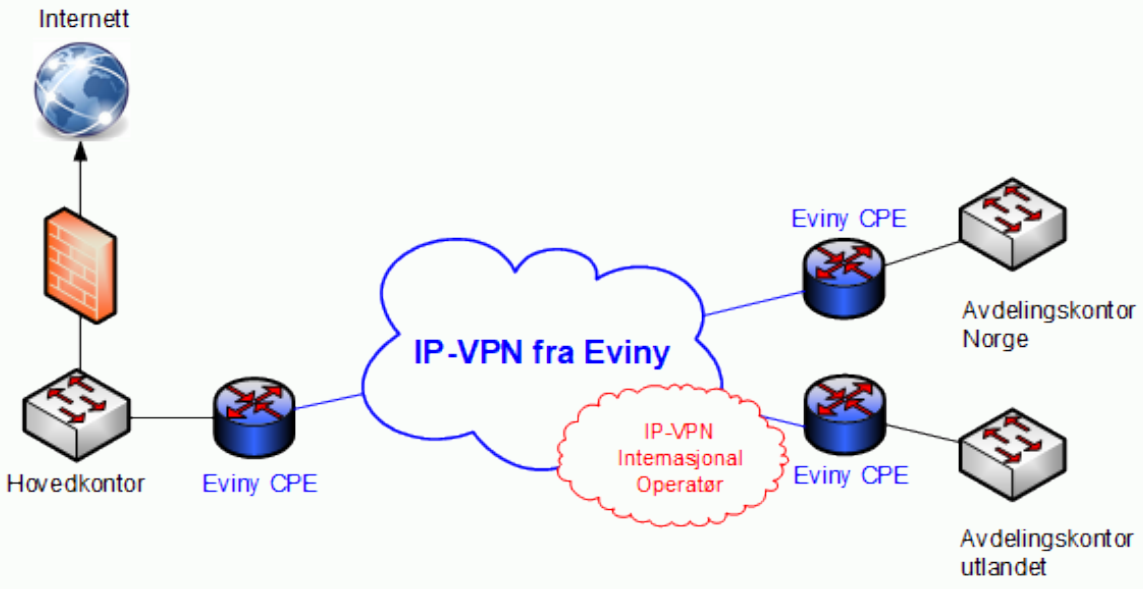
Service Level Agreement (SLA)

Eviny tilbyr tre servicenivåer Gull, Sølv og Bronse for alle tjenester. Bronse leveres som standard vederlagsfritt. For tjenester man ønsker et høyere servicenivå for, kan man velge enten servicenivå Sølv eller Gull.

Høyere servicenivå gir en bedre garanti for oppetid, raskere respons i feilsituasjoner, samt mulighet for feilhåndtering utover det som er normal åpningstid.

Internasjonalt IP-VPN

Eviny kan i samarbeid med andre internasjonale operatører tilby IP-VPN-samband til hele verden. Et slikt samband realiseres som et virtuelt dedikert samband for kunden, og blir ikke rutet over internett. Dette medfører en driftssikker og stabil tjeneste, siden Eviny og Evinys samarbeidspartnere har kontroll over nettverket fra ende til ende.

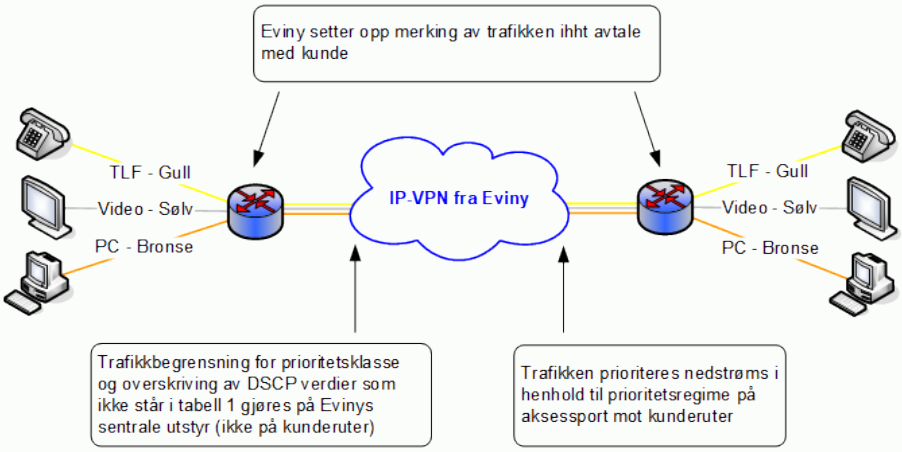


Tilleggstjenester

QoS

QoS kan benyttes hvis kunden har trafikktyper, applikasjoner og tjenester som er viktigere enn annen trafikk og som av den grunn må sikres mot pakketap og/eller jitter. Trafikk som merkes med en høyere prioritet blir prioritert og beskyttet gjennom nettet.

QoS kan leveres på samband levert på Evinys egen infrastruktur, og på samband der aksessen leveres via enkelte av Evinys underleverandører.



Merking av trafikk

Det tilbys tjenesteklasser som er basert på DSCP-verdi i pakken. De ulike trafikktypene merkes med klassens tilhørende DSCP verdi før de sendes inn i Eviny sitt nett, se tabell under.
Hvilken trafikk som skal klassifiseres i de ulike klassene må avtales mellom kunde og Eviny. Det finnes flere måter å klassifisere trafikken på. Dette avtales før QoS implementeres i IP-VPN tjenesten.

Vanlige metoder som benyttes for å merke trafikk og skille trafikktypene fra hverandre er:

- IP adresse
- TCP/UDP portnummer
- Protokoll (ved hjelp av NBAR, Network Based Application Recognition)
- Ingress fysisk og logisk port

All klassifisering foregår oppstrøms sett fra kunde (ingress på port på kunderuter).

Klasse	DSCP	Precedence	Eksempel på bruk
Gull	46 (EF)	5	IP telefoni
Sølv	32	4	Video, kritisk data
Bronse	24	3	Standard data
Best Effort	0	0	Internett trafikk

Prioritering av trafikk

All prioritering foregår nedstrøms sett fra kunde (egress på port på kunderuter). Prioriteringsmekanismene benytter seg av DSCP verdiene i pakkene og prioriterer basert på disse. Hvilke mekanismer som benyttes er plattformavhengig, men som hovedregelregel benyttes LLQ eller tilsvarende der plattformen støtter det.

Alle policyer benytter seg av følgende fordeling mellom klassene:

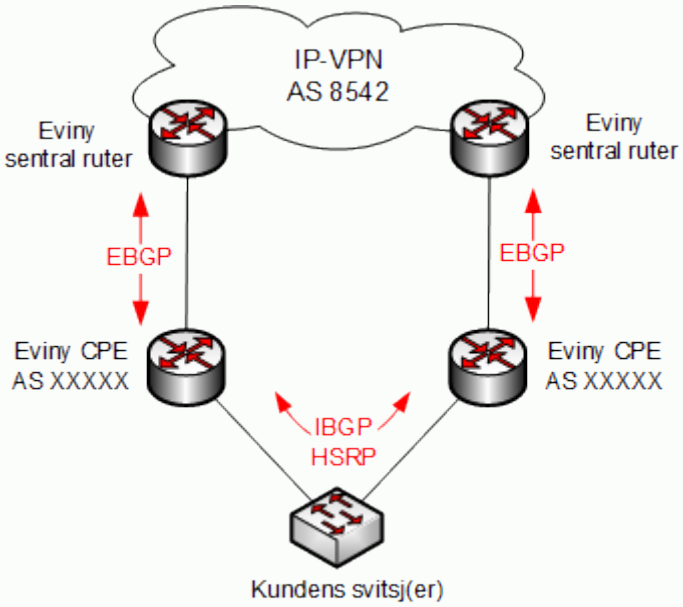
NB: Kunde kan i utgangspunktet sende inntil 40% av aksesshastighet i trafikklasse Gull inntil en øvre grense på 50 Mbit/s. Dersom 40% av aksesshastighet overstiger 50 Mbit/s settes denne til 50 Mbit/s.

Ta kontakt med Eviny for mer informasjon om QoS.

Klasse	Prioritet/Garanti	Merknad
Gull	PQ (Priority Queue)	All trafikk i denne kø sendes først uansett. Trafikk i klasse Sølv, Bronse og BE sendes først når alle pakker i klasse Gull er sendt.
Sølv	40% av resterende kapasitet	Garantert minimum 40% av resterende kapasitet etter at “Gull-klassen” har sendt det som skal sendes.
Bronse	40% av resterende kapasitet	Garantert minimum 40% av resterende kapasitet etter at “Gull-klassen” har sendt det som skal sendes
Best Effort	20% av resterende kapasitet	Garantert minimum 20% av resterende kapasitet etter at “Gull-klassen” har sendt det som skal sendes

IP-VPN Redundans

Eviny kan tilby redundans med to IP-VPN-linjer, for å sikre høyest mulig oppetid på sambandet. Redundans oppnås ved å etablere to uavhengige IP-VPN-linjer med diversitet til samme lokasjon, og etablere dynamisk ruting for automatisk failover ved brudd på den ene linjen. Eviny etablerer de to redundante IP-VPN-linjene på helt separate steder i Evinys nettverk, slik at en feil i én del av Evinys nettverk vil ikke påvirke begge linjene. påvirke begge linjene.



Kunderuter (CPE)

Eviny kan på forespørsel levere en komplett redundant løsning med to CPEer, for å sikre høyest mulig oppetid. CPEene er ferdig konfigurert med dynamisk ruting og automatisk failover.

Dynamisk ruting

BGP (Border Gateway Protocol) benyttes som dynamisk rutingprotokoll, og settes opp mellom CPEer hos kunde, og mellom CPEer og Evinys sentrale rutere, både på hovedlinje og backuplinje.

FHRP

Mellom Evinys CPEer, på LAN-siden, konfigureres FHRP (First Hop Redunancy Protocol) for å gi automatisk failover til backupruter hvis hovedruter skulle gå ned. For at FHRP og den redundante løsningen skal fungere, må Evinys CPEer kobles sammen via kundens lokalnett.

Som FHRP benyttes enten HSRP (Hot Standby Router Protocol) eller VRRP (Virtual Router Redundancy Protocol).

Som et alternativ til FHRP, kan det konfigureres dynamisk ruting mellom Evinys CPEer og Kundens utstyr.

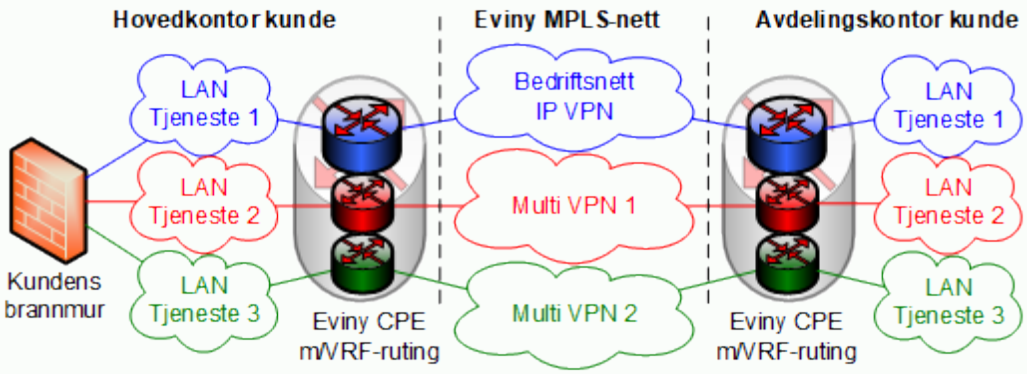
Automatisk failover ved brudd

Ruting-informasjon utveksles vha BGP mellom CPEene hos kunden og Evinys sentrale rutere. Den IP-VPN-linjen som er konfigurert som hovedlinje er foretrukket, og trafikken vil gå her i normalsituasjon. Ved et brudd på hovedlinjen vil trafikken automatisk legge seg over på backuplinjen. Når hovedlinjen kommer opp igjen, vil trafikken automatisk legge seg tilbake på den.

Konvergenstid (tiden det tar fra hovedlinje går ned til trafikken er lagt over på backuplinjen) vil variere avhengig av hvilken feil som oppstår, og hvor den oppstår. Maksimal konvergenstid vil være 30 sekunder.

Multi VPN

Multi VPN er et tilleggsprodukt til Bedriftsnett IP-VPN som kan benyttes hvis kunden har behov for å kjøre trafikk i et dedikert og adskilt nett. Trafikken i et VPN går helt adskilt fra trafikk i andre VPN. Dette gir kunden mulighet til å filtrere trafikk mellom ulike VPN i en sentral brannmur. På denne måten kan kunden bl.a sikre at sensitive data blir beskyttet, og at ulike sikkerhets- og tilgangspolicyer blir implementert for ulike deler av nettet sitt.



Med Multi VPN blir flere VPN konfigurert på samme fysiske linje ut til kunden, og båndbredde på sambandet deles mellom de ulike VPN. Hvis det er behov for økt båndbredde, må Bedriftsnett IP-VPN-sambandet oppgraderes med høyere båndbredde.

Multi VPN blir konfigurert som separate IP-VPN i Evinys MPLS-nettverk, og rutes i en egne VRF rutingprosesser på kunderuter. Trafikk mellom ulike nett er 100% adskilt. Multi VPN krever kunderutere som har støtte for VRF-ruting, og kan innebære behov for oppgradering av software på kunderuter.

Eviny tildeler WAN-adresser som benyttes mellom Evinys MPLS-nett og kunderuter. Kunden administrerer selv LAN-adresser på alle sine lokasjoner. Kunden får ved bestilling tilsendt et skjema som må fylles med informasjon bl.a om ønskede LAN-adresser. Utfylt skjema sendes til Evinys leveranseavdeling. Det kan konfigureres ruting av flere subnett i ulike VLAN på hver lokasjon. De ulike VLAN kan enten konfigureres på en 802.1Q trunk mot kundens utstyr, eller konfigureres på separate aksessporter hvis dette er tilgjengelig på kunderuter.

Multi VPN kan bestilles som tre ulike varianter:

- Multi VPN 5: Opp til 5 separate VPN
- Multi VPN 10: Opp til 10 separate VPN
- Multi VPN 25: Opp til 25 separate VPN

Tjenestebeskrivelse IP-VPN

eviny.no

Eviny AS
Postboks 7050,
5020 Bergen

Telefon: 55 57 00 00
E-post: hei@eviny.no