

## VPN: Valgets kvaler?

Se også "VPN+SSL: Enkelhet og sikkerhet" i Mellvik-Rapporten nr. 112.

*Det er klart vi bruker VPN. Det har vi hatt lenge. Men hvilken teknologi – eller hvorfor den ene i forhold til den andre? Se det er det langt verre å svare på. VPN er viktigere enn noen gang, men alternativene er ikke de samme som for 2 eller 4 år siden. Det er ikke bruksområdene eller behovene heller. For mange virksomheter er tiden overmoden for evaluering eller re-evaluering av behov, krav, alternativer, muligheter og ikke minst: Kostnader.*

"If it ain't broken, don't fix it" er et kjent og – for mange – kjært ordtak. I likhet med mangt annet, kan imidlertid også dette misbrukes og overdrives. Det faktum at vår 3 år gamle VPN-løsning ikke skaper problemer og synes å være både stabil og pålitelig, kan like godt være en illusjon som en realitet. Det er med VPN som med de fleste andre tiltak som helt eller delvis har med sikkerhet å gjøre: Den eneste måten å finne ut om de fungerer på, er å teste.

Dermed blir spørsmålet: "Når testet du din VPN-løsning sist?" Dessuten – selv om løsningen nylig er testet og godkjent, er poenget ovenfor gyldig: Dersom løsningen er mer enn 18 måneder gammel, er det nyttig med en gjennomgang – en kontroll av behov og krav i forhold til muligheter og priser.

### Alt beveger seg

Dersom vi plasserer oss selv i sentrum av universet og betrakter våre omgivelser, kan vi raskt konstatere at det meste er i bevegelse – også om vi kun tar for oss VPN og sikring av data 'in transit': Produkter, teknologi, tjenester, leverandører, behov, applikasjoner, brukere, forbindelser, båndbredde og priser. Observasjonen er så selvsagt at den knapt forårsaker et løftet øyenbryn. Samtidig er det vår oppgave å både kjenne til behovene og å vite hvilke muligheter som foreligger, ikke bare for å forbedre dagens situasjon funksjonelt eller sikkerhetsmessig, men også for å holde kostnadene der de hører hjemme.

Blant annet observerer vi at selv om mange har hatt VPN-løsninger som sikrer brukere 'på farten', i drift i lang tid, hører det til unntakene at de er problemfrie. Muligheter for forenkling og dermed bedre sikkerhet er derfor alltid interessante.

### En VPN-arkitektur

Når begrepet arkitektur kommer på banen, møter vi forbausende ofte negative reaksjoner: "Nei, vi trenger ingen arkitektur. Vi er små og har enkle, beskjedne behov." Årsaken er kun et mildt anslag av begrepsforvirring. 'Arkitektur' høres stort, ambisiøst og kostbart ut, mens 'plan' føles vesentlig bedre. I realiteten er det imidlertid en arkitektur vi trenger, uansett organisasjonens størrelse. En plan forteller hvordan og når målet skal nås, hvilket er viktig og nødvendig, mens arkitekturen beskriver målet. Begrepet 'arkitektur' sier ingen ting om størrelse eller kostnad, og kan i enkle tilfeller være nedfelt på et A4-ark. Den all-

VPN – Virtual Private Network

MPLS – MultiProtocol Label Switching

SSL – Secure Socket Layer

TLS – Transport Layer Security, det samme som SSL

IPSec – IP (Internet Protocol) Security [se Mellvik-Rapporten nr. 66]

tid like innlysende og lettglemte sannhet er at med mindre vi vet hvor vi skal, er enhver planlegging bortkastet.

### 3 alternativer

Vi har tre distinkte teknologi-alternativer til vår disposisjon når infrastrukturen skal transportsikres: MPLS, IPSec og SSL. Kun unntaksvis er forholdene så enkle at vi klarer oss med én av dem. Jo større og mer distribuert organisasjonen er, desto høyere er sannsynligheten for at alle tre varianter blir en del av arkitekturen. Uansett har valgene som gjøres, betydelige konsekvenser for fremtiden, fordi de påvirker hvilke veivalg som blir tilgjengelige lenger fremme.

Noen av de viktigste faktorene som må være med i evalueringen av teknologi og løsning, er:

- ✓ Skalerbarhet – for å kunne håndtere kontinuerlige endringer i krav og behov.
- ✓ Sikkerhet – uansett hvilke veier våre data transporteres, må vi vite at sikringen fungerer og er så god som foreskrevet.
- ✓ Tilgjengelighet – fordi vår avhengighet av infrastrukturen i mange tilfeller er total, ikke minst etter at telefoni ble en del av ligningen.
- ✓ Muligheter for trafikkstyring/QoS er ikke lenger kjekt å ha, men et krav, ikke bare for telefoni, men også for et voksende antall andre trafikktyper.
- ✓ Styrings/overvåkingsmekanismer: Det som ikke kan måles, kan heller ikke styres.

Nedenfor skal vi gjennomgå de tre teknologienes viktigste karakteristika, og i hvilke omgivelser/sammenhenger de kommer best til sin rett.

#### MPLS – MULTIPROTOCOL LABEL SWITCHING

MPLS har gått sin seiersgang gjennom store deler av telecom-industrien i løpet av de siste 4 årene, ikke bare på grunn av sine egenskaper, men fordi den dukket opp på riktig tidspunkt og raskt ble etablert som både leverandørnøytral og godt standardisert.<sup>1</sup>

MPLS hører hjemme i store nettverk – typisk hos ISPer og telecom-operatører, og er først og fremst våre dagers erstatning for tradisjonelle leide linjer og FrameRelay-forbindelser. Dermed er det primært store organisasjoner med ditto kommunikasjonsbehov mellom enheter, gjerne internasjonalt, som velger denne teknologien.

En MPLS-forbindelse mellom to eller flere punkter kan etableres på nettverksnivå (lag 2) eller på IP-nivå (lag 3), og gir den samme grad av sikkerhet og pålitelighet som tradisjonelle leide linjer. Siden slike forbindelser er dedikerte, og ikke en del av en offentlig (delt) infrastruktur (Internettet), får vi full kontroll over samtlige kvalitetsparametre. MPLS inngår typisk som en del av tjeneste-tilbudet fra teleoperatører – med følgende viktige karakteristika:

<sup>1</sup> Se artikkelen "MPLS: Universalmedisin for ustyrige IP-nettverk" i Mellvik-Rapporten nr. 97 for detaljer.

QoS – Quality of Service  
 CoS – Class of Service  
 SLA – Service Level Agreement

- ✓ Sikkerhet på nivå med leide linjer (ingen implisitt kryptering). Ingen andre har tilgang til eller ser vår trafikk.
- ✓ Full båndbredde-kontroll og dermed mulighet til å fordele og styre tilgjengelig kapasitet etter behov (QoS, CoS, SLA).
- ✓ Ansvar for linjer, drift og kvalitet er effektivt *outsourcet* – til telecom-operatøren.
- ✓ Høy skalerbarhet: Få reelle begrensninger med hensyn til antall tilkoblingspunkter og allokert båndbredde, begge deler kan justeres etter behov.
- ✓ Ute av syne for både brukere og IT-driftspersonell.
- ✓ Relativt høy kostnad.

### IPSec

IPSec kom sent, men godt, og har forlenget ridd av seg barnesykdommene, som blant annet skapte problemer i forbindelse med NAT, *Network Address Translation*. Som navnet indikerer, er dette en mekanisme for sikring av IP-trafikk, hvilket imidlertid ikke forhindrer IPSec i å transportere andre protokoller via såkalte tunneller.

IPSec kan benyttes overalt hvor IP brukes, og sørger for grunnleggende sikring av innholdet som transporteres – mot innsyn, endring, forfalskning av avsender og mot såkalte *replay attacks*.<sup>2</sup> Videre gir IPSec mulighet til å angi hvilken trafikk som skal beskyttes, hvordan den skal beskyttes og hvem som kan motta trafikken. Med IP som bærebjelke kan en nettverksarkitekt bruke IPSec til vilkårlige utvidelser av lokalnettet med Internettet som infrastruktur, hvilket naturlig nok også er IPSeCs viktigste bruksområde. Konfigurert riktig gir en slik struktur en grad av transportsikring som minst tilsvarer tradisjonelle leide linjer og MPLS, til minimale kostnader, spesielt over store avstander. Ulempen er naturligvis beskjeden kontroll over reell båndbredde og manglende muligheter for pålitelig prioritering av trafikk.

Mens IPSec kan brukes – og blir brukt – både i nett-til-nett og klient-til-nett sammenheng, er det førstnevnte som er mest interessant. Protokollen og de tilhørende mekanismene er generelt for kompliserte til å kunne eksponeres direkte overfor sluttbrukere – et forhold vi også har vært inne på ved tidligere anledninger. For hjemme-kontorer og småkontorer (SOHO), der en permanent ruter er kontaktpunkt mot Internettet, er IPSec et nærliggende valg.

IPSec-teknologiens sterke sider kan oppsummeres slik:

- ✓ Høyt sikkerhetsnivå: Sterke mekanismer legger til rette for brukerautentisering (autentisering av endepunktene), og beskyttelse av data – mot å bli sett og endret. Autentiseringen foregår med digitale sertifikater eller delte nøkler.

<sup>2</sup> 'Replay Attacks' er en form for angrep der legitime, krypterte datapakker tappes og gjenbrukes av en snok eller et program i et forsøk på å trenge gjennom sikringsmekanismene. Beskyttelse mot slike angrep krever blant annet nøyaktig tidsstempling av all trafikk.

- ✓ Kosteffektiv: Internettet er en billig og lett tilgjengelig infrastruktur, og IPSec støttes på et eller annet nivå i de fleste utstyrstyper, inklusive rutere for konsumentmarkedet.
- ✓ Enkel idriftsettelse: Vi kan gjøre det selv – om vi vil, uten å involvere ISP eller telecom-operatør. Det er også i mange tilfeller mulig å kjøpe hele tjenesten som en del av en pakke fra en ISP.
- ✓ En egenskap som kalles '*split tunneling*' gjør det mulig å splitte trafikken, slik at regulær Internett-trafikk ikke passerer gjennom den sikre kanalen, men går direkte til Internettet. Dette reduserer belastningen på sentrale tjenere, rutere og linjer vesentlig.

### SSL/TLS

SSL har tatt markedet med storm med sin enkelhet og sitt relativt høye sikkerhetsnivå. Disse to faktorene henger naturligvis sammen, i og med at høy kompleksitet er kjent for å redusere effektiviteten av selv de mest sofistikerte sikringsmekanismer. Her er også årsaken til at SSL har fortrenget vesentlig mer kompliserte alternativer – inklusive IPSec – fra deler av markedet for mobile brukere og hjemmebrukere.

SSL er innebygget i alle nettlesere, og krever ingen klientprogramvare utover dette. Den gir autentisering av partene og kryptering av trafikken dem imellom. SSL er en applikasjonsprotokoll, hvilket betyr at applikasjoner må modifiseres før de kan ta mekanismen i bruk. I utgangspunktet er dette en alvorlig begrensning, men i og med at nettleseren etterhvert blir hjemmemiljø for stadig flere applikasjoner, reduseres begrensningen over tid. Nettleseren sørger for sikringen, uten at applikasjonene merker noe til det. Videre dukker SSL-støtte opp i stadig nye sammenhenger, slik at for eksempel epost i dag gjerne kan både hentes og leveres via SSL, uten å gå veien om nettleseren.

En annen faktor som har bidratt til interessen for SSL på bekostning av for eksempel IPSec, er at sikring på applikasjonsnivå gjør det mindre kritisk hvilke andre programmer, tjenester og forbindelser som måtte være aktive på samme klient. Med andre ord kan SSL gi adekvat sikkerhet også på klienter som er utenfor kontroll – for eksempel Internett-kiosker og offentlige maskiner på messer, i hotell-lobbyer og Internett-kaféer.

SSLs sterke sider kan oppsummeres i følgende punkter:

- ✓ Enkelhet – finnes over alt, veletablert kompatibilitet og sikkerhet, ingen brukerterskel.
- ✓ Tilstrekkelig fleksibel til å kunne støtte nye autentiseringsmekanismer som måtte bli introdusert i fremtiden.
- ✓ Billig å ta i bruk og å bruke.
- ✓ *Transparent roaming* – verken sikkerhetsmekanismer eller forbindelse er knyttet til IP-adresse, slik at en bruker kan flytte seg fra nettverk til nettverk uten å miste (den logiske) forbindelsen.

## Konklusjon

Forbausende ofte møtes en presentasjon av valgmuligheter med interesseløshet og skepsis. "Nå blir det enda mer komplisert." Mens en slik reaksjon kanskje kan forklares, kan den sjelden eller aldri forsvares. Alternativer betyr alltid muligheter – til å finne løsninger som stemmer bedre overens med behov og budsjett.

I tilfellet VPN er det sågar slik at de tre variantene vi har presentert, kun i beskjeden grad overlapper hverandre. Til sammen spenner de over et spekter av behov som ingen av dem kan dekke alene. For oss som skal definere og implementere en VPN-arkitektur, betyr kunnskapen om hva som passer hvor, at vi har grunnlaget – som kombinert med en behovsanalyse setter oss i stand til å gjøre riktige valg. ■