

VPN+SSL: Enkelhet og sikkerhet

Stoff om VPN i tidligere utgaver av Mellvik-Rapporten:

- “VPN: Sikre øyer på utrygt hav” i nr. 52
- “VPN: Penger å spare, penger å tape”, artikkelserie i 5 deler med start i nr. 58.
- “IPsec: Sikkerhet på overtid for TCP/IP” i nr. 66

L2TP – Layer 2 Tunneling Protocol

PPTP – Point-to-Point Tunneling Protocol

Fjernaksess handler om tilgang til tjenester og data ‘utenfra’. VPN⁵ og tilhørende krypteringsmekanismer skal sørge for at slik tilgang er sikret, både med hensyn til autentisering av brukeren og å gjøre dataoverføringene utilgjengelige for innsyn. En VPN-løsning har dessuten en rekke andre sikkerhetsrelaterte oppgaver som ikke er mindre viktige, men som har lett for å komme i bakgrunnen.

Allerede i 1998 ble VPN-teknologi utropt til Internettets nye ‘killer-app’, en katalysator for ny akselerasjon i bruken av Internettet. Eksplosjonen har riktignok ikke blitt så voldsom som mange hadde håpet, men VPN er forlenget blitt en selvfølge – og en forutsetning for jevnt voksende bruk av hjemmekontorer og konnektivitet for brukere på farten.

Protokoller og tunneller

Et grunnleggende element i alle VPN-varianter er ‘tunneller’ eller ‘virtuelle nettverksforbindelser’. Begrepet går igjen i navnene på de mest utbredte protokollene for 1. generasjons VPNs: L2TP og PPTP. Disse er fortsatt i bruk, men er plaget av både praktiske og sikkerhetsmessige begrensninger som gjør dem mindre egnet i større sammenhenger. Dessuten, og like viktig, finnes det andre alternativer som er mer attraktive. På teknologi-nivå er IPsec – IP Security – den viktigste, i kraft av sin utbredelse og sin sikkerhetsmessige styrke. IPsec ble en praktisk realitet i 1999 og har vært generelt tilgjengelig i systemer og nettverksprodukter siden 2000 (se Mellvik-Rapporten nr. 66 for en gjennomgang av IPsec).

Felles for denne gruppen protokoller (IPsec, PPTP, L2TP og flere) er at de opererer på link- eller transport-nivå. De integreres i selve infrastrukturen og er transparente for såvel brukere og som applikasjoner. Graden av usynlighet for brukeren avhenger riktignok av både implementasjon og system. De fleste IP VPN-produkter som installeres direkte på klient-maskiner, forutsetter betydelig deltagelse fra brukeren i autentiseringsfasen.

Kravet til transparens har vært en forutsetning for å kunne introdusere sikkerhet uten å foreta dyptgripende forandringere i eksisterende miljøer og systemer. Mens sikring på applikasjonsnivå alltid har vært ønskelig, har det også vært en praktisk umulighet. VPN-mekanismene har kort og godt gitt god sikkerhet uten å introdusere vesentlig kompleksitet – i alle fall på papiret.

5 Det finnes ingen entydig definisjon av begrepet VPN. Den mest alminnelige, som også brukes av oss i denne sammenheng, er: “Et VPN etablerer en tilsynelatende direkte forbindelse mellom to eller flere endepunkter via et offentlig nettverk, og med sikkerhetsmekanismer for autentisering, kryptering av trafikk, mm.”

Utvikling og forandring

IPsec kom markedet til unnsetning på et viktig tidspunkt, og ble den VPN-standarden vi trengte. Verden står imidlertid ikke stille. Krav og behov forandrer seg, og praktisk erfaring påvirker oppfatningen om hva som er mulig og optimalt. Forandringenes vind blåser spesielt kraftig over VPN-markedet i disse dager.

Hva er i veien med IPsec?

Så sent som for et års tid siden var IPSec-baserte VPN-løsninger – ofte betegnet IP VPN – det selvfølgelig valg i profesjonelle sammenhenger utover minimums størrelse. Både nett-til-nett og klient-til-nett scenarier kunne håndteres med lett tilgjengelige produkter fra praktisk talt alt som kan krype og gå av leverandører i markedet. Med velprøvde implementasjoner på de fleste systemplattformer og støtte fra Internettets standardiserings-organ IETF, ga valget seg i mange tilfeller selv.

De siste års erfaringer har imidlertid vist at IPsec ikke er noen univertsalmedisin for alle tenkelige situasjoner. Tvert imot dukker det stadig oftere opp scenarier der IPsec enten blir for tung og komplisert, eller rett og slett er feil løsning i forhold til oppgaven. Her er en oppsummering av de viktigste innvendingene og svakhetene:

- ✓ IPsec er laget for høy sikkerhet og ditto fleksibilitet. Standarden spesifiserer en rekke alternative mekanismer for kryptering og utveksling av krypteringsnøkler, og åpner sågar for introduksjon av nye slike mekanismer. Leverandørene kan selv velge hvilket eller hvilke av alternativene de vil implementere – med den følge at produktene ikke nødvendigvis kan snakke sammen. Problemer med samspill på tvers av leverandører har plaget IPsec siden de første produktene kom på markedet.
- ✓ Likeledes har utveksling av krypteringsnøkler vært en utfordring av betydelige proporsjoner. Når IPsec kjøres direkte på brukernes (ofte bærbare) klienter, blir brukeren selv involvert i prosessen, hvilket både blir en komplikasjon og en potensiell kilde til kompromittering av sikkerheten. Videre bidrar komplisert nøkkelutveksling til å redusere teknologiens skalerbarhet og å øke belastningen på driftspersonell.⁶ Den samme kompleksiteten fører til produkter som er kostbare både i anskaffelse og drift.
- ✓ IPsec er laget for å gi en transparent, sikret forbindelse mellom nettverkene som kobles sammen. Mens det naturlig skal foretas trafikkfiltrering for å holde unna uønsket trafikk i den ene eller begge ender, impliserer denne åpenheten at endepunktene må være skikkelig sikret. Denne forutsetningen kan tilfredsstilles når avdelingskontorer eller større enheter

⁶ Det finnes verktøy som skal håndtere (gjemme) denne kompleksiteten (se for eksempel rapporten 'EASYVPN: IPSEC REMOTE ACCESS MADE EASY' fra Columbia University, som nylig ble presentert på en driftskonferanse i California [<http://www1.cs.columbia.edu/~angelos/Papers/easyvpn.pdf>]). I den forbindelse er det interessant at de beste (enkleste) verktøyene benytter SSL/TLS for utveksling og administrasjon av nøkler. Dette er vel og bra, men kan ikke unngå å aksentuere spørsmålet om hvorfor SSL/TLS ikke like godt kan gjøre hele jobben.

tilhørende samme organisasjon kobles sammen, men er en umulighet for enkeltklienter, enten de befinner seg *on the road* eller på hjemmekontor. Da blir brukeren selv ansvarlig for sikkerhetsnivået, som blir deretter.

- ✓ Bruk av NAT – *Network Address Translation* – for Internett-tilknytning er blitt regelen for både privat- og bedriftsmarkedet de siste årene. NAT er nødvendig for å redusere forbruket av et begrenset tilfang av offisielle Internett-adresser, og har dessuten en rekke sikkerhetsmessige fordeler. Samtidig skaper den problemer for IPsec. Problemene er håndterbare, men løsningen betyr en ytterligere omdreining på kompleksitets-skruen, hvilket aldri er positivt for sikkerheten.

IPsec er kort og godt ikke den universalmedisinen mange hadde håpet og regnet med. Alle sine gode egenskaper til tross er teknologien komplisert, kostbar, lite fleksibel og sist men ikke minst: Den stiller krav til brukermiljøene som er vanskelige eller umulige å tilfredsstille. Det siste gjelder spesielt for individuelle klienter. Selv med restriktive regler for bruk og grundig opplæring av brukerne, vil en bærbar maskin og et hjemmekontor alltid representere en ukvantisert risiko som vi fortrinnsvis vil unngå å innlemme i det interne nettverket.

SSL inn fra sidelinjen

SSL – *Secure Socket Layer*, opprinnelig utviklet av Netscape, nå en Internett-standard under det misvisende navnet TLS. SSL og TLS er med andre ord to sider av samme sak.

TLS – *Transport Layer Security*
Navnet er misvisende fordi dette i virkeligheten er sikring på applikasjonsnivå, ikke på transportnivå.

Innvendingene er ikke nok til å gjøre IPsec uinteressant, men mer enn tilstrekkelig til å trigge interessen for andre alternativer. På sett og vis har vi rykket tilbake til start: Før VPN ble en teknisk realitet, sto applikasjonssikring øverst på ønskelisten, men lot seg ikke realisere. Tunnel, kryptering og VPN-produkter kom til unnsetning, og brakte oss til neste nivå. I dag ser bildet annerledes ut. Applikasjonssikring er innen rekkevidde – takket være SSL-teknologien, som har sørget for sikkerhet i våre nettlesere siden midten av nittitallet. Nyanseringen bidrar til at IPsec-basert VPN-teknologi finner sin riktige plass i nettverket: Som sammenkoblingsteknologi mellom nettverk – som hver på sin side er sikret, og i relativt statiske omgivelser.⁷

Enkel og tilgjengelig

SSL er allesteds nærværende, enkel, fungerer uten innblanding fra brukerne, og er tilstrekkelig sikker for de fleste alminnelige formål. Teknologien er blitt stuevarm i den grad at en hel verden daglig eller ukentlig handler på Internettet uten å reflektere over sikkerheten utover å konstatere at et låslignende symbol dukker opp i kanten av nettleseren.

⁷ En beslektet diskusjon som gjerne dukker opp i denne forbindelse er hvorvidt dedikerte, leide samband trenger den ekstra sikkerheten VPN gir, eller om slike private forbindelser virkelig er private. Svaret avhenger av en rekke faktorer – for eksempel: Hvilken teknologi benytter telecom-leverandøren for å skille trafikk fra ulike kunder i sitt stamnett, hvilken tillit har vi til leverandøren, hvilke garantier gir leverandøren og hvor følsomme er dataene som skal transporteres? Tradisjonelle leide linjer, Frame Relay og ATM er på full fart over i historien, og avløses av IP og MPLS – selv i internasjonale stamnett. Kombinasjonen gir sikkerhet på linje med teknologiene den avløser, et forhold vi diskuterte i MPLS-artikkelen i Mellvik-Rapporten nr. 97.

En jevnt voksende andel av både profesjonelle og private brukeres aktiviteter foregår via nettleseren. Å sikre aktivitetene med SSL representerer en beskjeden kostnad, fordi teknologien allerede finnes både på klient- og tjenersiden, og dessuten er velkjent og velprøvd. Å sende denne sikrede datastrømmen gjennom en ekstra VPN-forbindelse blir det vi gjerne kaller 'smør på flesk': Komplisert, ressurskrevende og unyttig.

Et annet forhold som lett glemmes i vår streben etter høyere sikkerhet, er at en betydelig del av nett-surfing og enkelte andre aktiviteter for brukere flest ikke har behov for sikring. Å lese aviser, fagstoff, produktinformasjon og deltagelse i faglige fora fordrer ingen spesielle sikkerhetstiltak.

Mens nettleserens voksende rolle er den lettest synlige drivkraften i denne utviklingen, er den ikke den eneste. Sentraliserings-bølgen som har skyllet over markedet de siste årene, er en vesentlig faktor i seg selv. For eksempel har Windows Terminal Server løsninger i kombinasjon med Citrix MetaFrame og omkringliggende teknologier sine egne sikringsmekanismer på applikasjonsnivå, som for alminnelige anvendelser gir tilstrekkelig sikkerhet – etter samme prinsipp som kombinasjonen SSL og nettleser: Applikasjonssikring.⁸

Essensen i disse observasjonene er at sentralisering av tjenester og konvergering mot nettleseren som brukergrensesnitt, åpner for enklere og mer oppgavetilpassede sikringsmekanismer enn tradisjonell VPN-teknologi har kunnet tilby. Innenfor rammene av nettleseren kan vi både sørge for bruker-autentisering og sikring av datastrømmen etter behov. Faktum er at slik autentisering i et voksende antall tilfeller er en del av prosessen allerede, gjennom IEEE 802.1x standarden, som er helt eller delvis på plass i moderne trådløse aksesspunkter/svitsjer og annet sammenkoblingsutstyr.

Ingen gratis lunsj

Om SSL er aldri så allesteds nærværende, kommer sikkerheten fortsatt ikke av seg selv. Forenklingseffekten i forhold til tradisjonell IP VPN kommer først og fremst på klientsiden: En moderne, fullfunksjons nettleser er alt som skal til for å komme i gang. På tjenersiden vil den voksende belastningen føre til at ekstra hardware må anskaffes, ikke bare for SSL-prosesseringen, men også for autentisering (typisk via 802.1x-standard) og andre oppgaver som vi kommer tilbake til nedenfor.

Likeledes fører bruken av nettleser og SSL med seg en serie nye utfordringer – av såvel praktisk som sikkerhetsmessig art. For eksempel blir det ofte påpekt at ende-til-ende sikring (applikasjon-til-applikasjon) fjerner muligheten til å foreta effektiv innholdskontroll av datastrømmen. Kryptert innhold kan aldri kontrolleres. Dette er én av utfordringene de relativt ferske SSL-baserte VPN-boksene på markedet

⁸ Som levert fra Microsoft og med Microsofts RDP-klient, gir Windows Terminal Server ingen sikring utover selve påloggingen.

skal ivareta. Dekrypteringen – og fortrinnsvis innholdskontrollen – må skje før vi kommer inn i det interne nettverket.

Videre har erfaring med første generasjons SSL VPN-produkter avslørt en rekke andre svake punkter som må håndteres. De viktigste er:

- ✓ Web-baserte brukergrensesnitt til for eksempel epost har gjennomgått dramatiske ansiktsløftninger både utseendemessig og funksjonelt det siste året. Behandling av vedlegg nødvendiggjør imidlertid nedlasting av data til klienten – for lesing og eventuell modifikasjon. I utgangspunktet har vi liten eller ingen kontroll over hvor disse dataene havner og om/når de slettes.
- ✓ Antall applikasjoner som er tilpasset Web-omgivelsene er fortsatt beskjedent. For å omgå dette problemet, er det utviklet en rekke ActiveX- eller Java-programmer som kanalisierer (omdirigerer) datastrømmen mellom klient og tjener til å passere gjennom nettleseren og dermed SSL. Mens dette kan høres tilforlatelig ut, er det også en måte å lure seg selv på. Brukt på denne måten spiller SSL den samme rollen som tradisjonell IP VPN-teknologi, med de samme utfordringene.

Disse punktene er viktige når sikringsteknologi skal evalueres i dag. Feilen mange har gjort både i forbindelse med IP VPN og første generasjons SSL VPN, er å betrakte dem som universalløsninger for alle slags fjernaksess-typer. Det verken er de eller blir de. Her som i andre sammenhenger må løsningen tilpasses til oppgavene, og vi kan gjøre følgende observasjoner i tilknytning til SSL-baserte VPN-løsninger:

- ✓ Brukerne må holdes innenfor rammene av nettleseren. Slik utviklingen går, blir denne 'restriksjonen' mindre betydningsfull måned for måned, blant annet takket være *Web-services* (se Mellvik-Rapporten nr. 110).
- ✓ Utstyret vi anskaffer på tjenersiden må – i tillegg til å ha god kapasitet for kryptering/dekryptering av datastrømmen samt autentisering mot eksisterende katalogtjenester, gi muligheter for både innholdskontroll og styring av aktiviteter i henhold til policy. De mest sofistikerte produktene kan gi ulike brukergrupper forskjellige privilegier i så henseende.⁹
- ✓ Dynamisk sikkerhetsnivå: Virkeligheten tilsier at spredningen – funksjonelt og sikkerhetsmessig – mellom ulike brukerteminaler vokser. Derfor må utstyret på tjenersiden være i stand til å justere grensene for hva som tillates i henhold til hva brukerutstyret kan håndtere. For eksempel er det mulig å 'fjernundersøke' innstillingene på nettleseren, forandre dem og kontrollere på nytt, og deretter avgjøre hva brukeren får lov til.

⁹ I en test som nylig ble utført av fagbladet *Network Computing*, fikk SSL-produktet *Access Series 5000* fra selskapet *Neoteris Inc.* et spesielt godt skussmål. *Neoteris* [www.neoteris.com] ble nylig oppkjøpt av en annen aktør i dette segmentet, *NetScreen Inc.* Pekere til denne testen, som også tar for seg en rekke andre produkter, samt annet relatert materiale, finner du på tilleggsstoff-siden på vår Web-tjeneste, se side 35.

Det sier seg selv at dette blir forskjellig på et hjemmekontor i forhold til en Internett-kiosk eller en mobiltelefon/PDA.

Konklusjon

Uttrykket SSL VPN er egentlig misvisende og skaper inntrykk av at funksjonen tilsvarer 'tradisjonelle' IP VPN-løsninger. Den gjør ikke det, og erstatter dem heller ikke. **Tilveksten av SSL-baserte løsninger har forenklet sikringen av små nettverk og mobile klienter, og har samtidig henvist IPsec-baserte løsninger dit de hører hjemme.** Dette kalles bedre oppgavetilpasning og representerer en forenkling for alle parter i markedet.

De beste SSL-baserte løsningene er ikke rimeligere i anskaffelse per bruker enn IP VPN-løsninger, men gir bedre totaløkonomi fordi drifts-omkostningene reduseres og sikkerheten bedres. ■