Virtual Private Network

Protokoller og sikkerhetsmekanismer

Hovedoppgave
ved
sivilingeniørudanning i
informasjons- og kommunikasjonsteknologi

av
Bodil Rønbeck Johansen

Grimstad, juni 1999

Sammendrag

Dette dokumentet beskriver hvordan Internett kan brukes som et sikkert underliggende transmisjonsmedium for bedriftsintern kommunikasjon eller kommunikasjon mellom samarabeidspartnere. For å realisere en slik sikker kommunikasjon har man utviklet et konsept kalt Virtual Private Networks (VPN). Vil på ulike måter, beskrive bakgrunnen for VPN, hva VPN er og hvordan det brukes. Kommer videre inn på hvilke protokoller og sikkerhetsmekanismer som brukes for å realisere en slik løsning, og beskriver i detalj hvordan disse er bygget opp.

Å sikre informasjon som utveksles har i mange sammenhenger betydd å gjøre informasjonen uleselig og usynlig for andre enn den som informasjonen er ment for. Slik er det også i forbindelse med VPN hvor kryptering er en vesentlig del. Hvilke krypteringsmetoder som brukes blir omtalt, og detaljene kan leses på viste linker.

Det finnes flere produkter på markedet som kalles VPN-løsninger, men her er valgt å gi en oversikt over to VPN produkter hvor krypteringsmekanismen foregår i hardwaren. Disse to produktene blir sammenlignet, og tester som er gjort på disse to produktene omtaltes. Har også tatt med momenter som en må ha med ved valg av en eventuell VPN-løsning i en organisasjon.

Tilslutt har jeg referert fra en case-studie gjort hos et firma som har avdelingskontorer og brukere, spredt rundt hele verden. Disse har behov for tilgang til informasjonssystemene på hovedkontoret.

Har ikke kommet inn på detaljer rundt det økonomiske aspektet. Omtalte tekniske løsninger som ikke er beskrevet i detalj, kan for interesserte finnes på viste referanser.
Det er forutsatt at leseren kjenner til vanlige begreper som brukes innen IT-sikkerhet, datakommunikasjon og IP (Internet Protocol).

Innholdsfortegnelse

1. Innledning

Internett teknologien har medført forandringer på hvordan bedrifter og organisasjoner utveksler informasjon med sine kunder, medarbeidere og samarbeidspartnere. Hittil har de fleste vært svært forsiktige med hvilken infomasjon som utveksles via Internett, og det har stort sett vært informasjon som ikke innebærer noen sikkerhetsrisiko eller informasjon som allerede er offentliggjort via andre media.

I det siste er flere og flere blitt klar over at det går an å bruke Internett som et mellomledd for sikker og mer kostnadseffektiv informasjonsutveksling. Det er derfor økende interesse og tilslutning til at adgangen til f.eks. ordre status, lagerbeholdning eller økonomisk og bedriftsensitiv informasjon kan skje gjennom Virtual Private Network (VPN).

2. Hva er VPN?

Et VPN er kjent som en kommunikasjonsløsning som sikrer private forbindelser ved å bruke et ikke-sikkert medium. Det finnes utallige definisjoner og beskrivelser på VPN. En enkel og klar definisjon av VPN er ikke lett å finne, men en formell karakteriseringen av VPN er denne:

”Et VPN er et kommunikasjons miljø, eller løsning, hvor tilgangen er kontrollert for å tillate kommunikasjon mellom to eller flere parter, bare innenfor et definert interessefellesskap som er konstruert gjennom en form for deling av et felles underliggende kommunikasjonsmedium, hvor dette underliggende kommunikasjonsmediet er alment tilgjengelig.”[1]

2.1 Hva betyr ordene Virtual Private Network ?

En annen måte å beskrive VPN på, er å beskrive hva som menes med hvert enkelt ord i VPN.

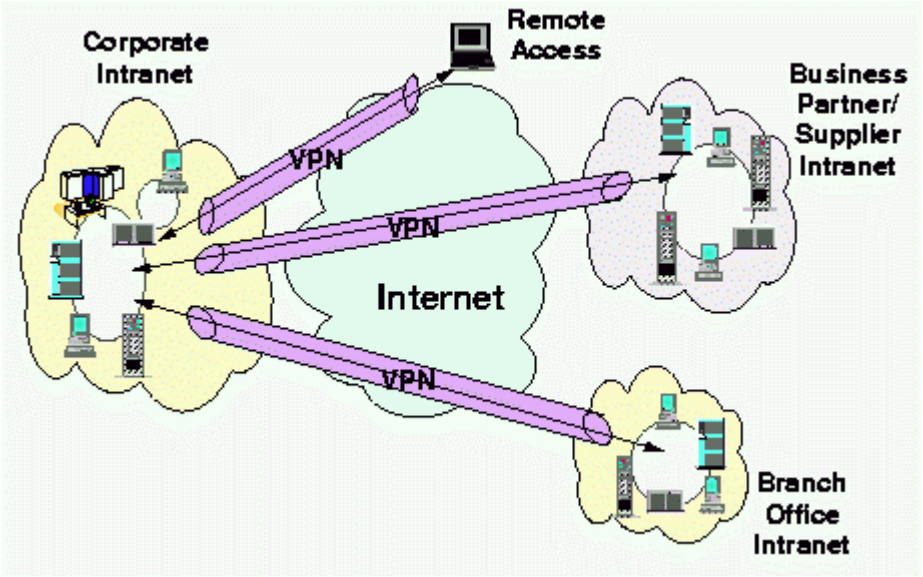
Network: Et nettverk består av et antall enheter som kan kommunisere på en vilkårlig måte.

Private: Med privat menes at kommunikasjon mellom en eller flere enheter er sikker. Med det menes at enheter som ikke er deltagere i kommunikasjon ikke har tilgang til innholdet, og at disse ikke-deltagerne er fullstendig uvitende om at kommunikasjon mellom de private enhetene foregår.

Virtual: simulerer en funksjon som i virkeligheten ikke er tilstede. Her betyr det at deltagerne i kommunikasjon oppfatter det som om de kommuniserer over et eget fysisk nett, mens kommunikasjon foregår over et offentlig tilgjengelig underliggende nettverk. Det underliggende nettverket, som altså er delt av mange, kan f.eks. være Internett.

2.2 VPN i dette dokumentet

Et virtuelt privat nettverk (VPN) er en temporær sikker forbindelse som benytter et offentlig tilgjengelig nett som det underliggende nett, og har en oppbyggning som vist på Figur 1. Hovedvekten legges på et VPN som realiseres ved bruk av IP (Internet Protocol).



Figur 1: Virtuelt Privat Nettverk (VPN)

3. Private nettverk

Den økende interesse for bruken av Internett som et underliggende nettverk, istedenfor eksisterende private nettverk, kommer fra ønsket om en mer kostnadeffektiv måte å bygge, og gruppere private nettverk, for kommunikasjon mellom virksomhetens lokasjoner.

3.1 Eksisterende Private Nettverk

Inntil nylig kunne eksisterende nettverk beskrives som:

3.1.1 Dedikerte WAN (Wide Area Network)

I et dedikert WAN er de forskjellige fysisk delte lokasjonen forbundet permanent opp med hverandre. WAN er implementert ved hjelp av leide linjer eller dedikerte nettverk, som for eksempel Frame Relay eller ATM. Virksomhetens private rutere eller switcher på de forskjellige lokasjonene knytter nettene sammen og sørger for kommunikasjon mellom lokasjonene.

3.1.2 Oppringte nettverk

Ved oppringte nettverk opprettes forbindelsen etter behov via telefonnettet til en eller flere av virksomhetens private nettverk. Normalt opprettes forbindelsen ved å bruke en vanlig analog telefonlinje eller ISDN som ringer opp en modem-pool eller en ISDN-router som videre er knyttet mot en server (NAS - network-access-server/RAS – remote access server).

3.2 Virituelle Private Nettverk

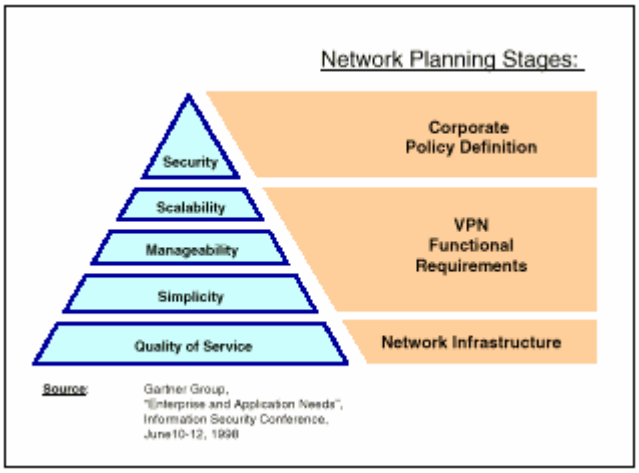
Virksomheter som har medarbeidere plassert på forskjellige fysiske lokasjoner har sett behov for en mindre ressurskrevende kommunikasjonsløsning enn overstående. Derfra er tanken om VPN og bruk av Internett som underliggende nett, utviklet seg.
Et VPN kan deles inn i flere typer, og har som formål å dekke følgende kommunikasjonsbehov [2]:

- mellom en virksomhets kontorer og virksomhetens reisende eller tilfeldig plasserte medarbeidere og kan benevnes som "remote access VPN".
- mellom en virksomhets hovedkontor og dets avdelingskontorer, som kan kalles et "intranett VPN".
- mellom en virksomhet og den samarbeidspartnere (leverandører, kunder eller investorer), "ekstranett VPN".

De forskjellige typene VPN beskrives mere detaljert i kapittel 6: Forskjellige typer VPN.

4. Krav til et VPN

For illustrasjon viser Figur 2 en 5-lags modell som Gartner Group har publisert. Modellen skisserer momenter man bør ta med under planlegging av en organisasjons VPN løsning [3].



Figur 2: Krav til VPN fra Gartner Group

For et VPN basert på et underliggende IP nettverk vil disse kravene generelt omhandle ([4] og [5]):

- **Støtte for ugjennomtrengelig pakke transport:**
  Informasjonsutvekslingen som foregår innefor et VPN skal ikke ha noen relasjoner til det underliggende IP nettverket. Med det menes at det interne nettverket skal være skjult, og ikke på grunn av at flere protokoller kan bæres i et VPN, eller fordi en kundes private IP-nettverk bruker adressering som ikke er relatert til det underliggende IP-nettet hvor trafikken transporteres. Med det siste menes at kunden bruker privat IP-adressering som ikke er unik i Internett sammenheng.

- **Støtte for data sikkerhet:**
  Generelt krever brukere av VPN en form for data-sikkerhet utfra den vanlige oppfatningen rundt mangel på sikkerhet i IP nettverk, og spesielt på Internett. Det tenkes da ofte på angrep rettet mot svakheter i TCP/IP [6], at pakker adresseres feilaktig, at pakkene ikke skal forandres eller muligheter for andre til å putte uautoriserte pakker i sendingen. Om disse antagelser er riktig eller ikke, så må sikkerhet være et hovedmål med en hver VPN implementasjon.

- **Støtte for tjenestekvalitet:**
  I tillegg til sikring av privat kommunikasjon, tilbyr eksisterende nettverk som er bygd på fysisk- eller link-lag mekanismer, varierende typer av tjenestekvalitets garantier. Leide linjer og oppringte forbindelser tilbyr både båndbredde og forsinkelses garantier, mens dedikerte forbindelser som ATM og Frame Relay har omfattende mekanismer for tilsvarende garantier. Ettersom IP baserte VPN blir mer utbredt, vil det bli et marked for behov av lignende garantier.

  Mens mulighetene til å tilby tilsvarende garantier for VPN basert på IP, avhenger mye av samsvarende muligheter i det underliggende IP-nettverket. Kravene til tjensestekvalitet for et VPN må derfor også omfatte det underliggende nettverket, som VPN benytter, og slike muligheter er hele tiden under utvikling. Blant mange, har Cicso System utarbeidet et ”white paper” [7] som omtaler tjenestekvalitet basert på bruk av ”Type of Service” feltet i IP-headeren, og oppdaterte linker om temaet er utarbeidet av Ohio StateUniversity Department of Computer and Information Science [8].

- **Administrasjon:**
  Et VPN bør sees i sammenheng med virksomhetens overordnede sikkerhets filosofi, hvilke tilpassning- og utvidelsesmuligheter som finnes og videre at løsningen krever lite ressurser til drift og administrasjon.

De første to kravene forusetter at VPN må implementeres via en type IP-tunneling mekasnisme, hvor pakkeformat og/eller adresseringen som brukes innen VPN'et ikke må relateres til bruk ved ruting av pakkene i tunnelen over det underliggende IP-nettet. Slike tunneler , avhengig av deres form, kan støtte noen nivåer med reell datasikkerhet, eller dette kan også oppnås ved forsterket bruk av andre mekanismer (f.eks. IPSec [9])

5. Sikkerhetsmomenter som bør løses ved VPN

Mange leverandører av VPN tilbyr autentisering og kryptering, men for å garantere sikkeheten på en nettverksforbindlelse må følgende tre teknologier være ivaretattt: autentisering av brukerne, intergritet og hemmeligholdelse av infomasjonen.

- **Access Control/tilgangskontroll:**
  Brukere av et VPN kan inkludere: ansatte, samarbeidspartnere, kunder og leverandører. Access Control et nøkkelkrav hvor hver bruker har autorisasjon til å komme inn på spesifiserte deler av informasjonen på nettverket.
  Et VPN uten aksess kontroll vil bare sikre dataene mens de sendes over transportmediet. Aksess kontroll beskytter ikke bare dataene. Siden VPN-brukere bare har full aksess til de applikasjoner og informasjon som de trenger, og ikke mer, ivaretar man også virksomhetens "fullkomne rikdom av intellektuell eiendom" og informasjon.

- **Authentication:**
  Det finnes to typer autentisering som er brukt i VPN implementasjoner: bruker authentisering og autentisering av data.
  Data autentisering sikrer at meldinger er sendt av den som utgir seg for å være senderen og har den samme form når den ankommer mottakeren som den var når senderen sendte den.
  Bruker autentisering er prosessen som skal til for å verifisere at senderen virkelig er den han eller hun gir seg ut for å være.

  Begge typene av autentisering er viktig for en virksomhet som er spredt geografisk og bruker VPN. En omfattende VPN løsning må ha både data og bruker authentisering.

  Bruker-autentiserings systemet bør ha mulighet for "to-trinns" autentisering. To-tinns autentisering gir en mer enn dobbel sikkerhet i forhold til den vanlige brukernavn/passord, siden et to-trinns autentisering system krever to elementer: brukernavn/passord og f.eks. en PIN kode eller et elektronisk merke som kan være et ID-kort. Brukeren må da være i besittelse av et kort og samtidig huske sitt passord. Dette vil dramatisk redusere mulighetene for uvedkommende å komme inn på et nettverk.

- **Encryption/Kryptering:**
  Kryptering stokker om på dataene slik at bare de som har nøkkelen til å lese informasjonen har mulighet til å dekode meldingene. Krypteringsfunksjon bør være tilgjengelig med en gang en bruker blir autentisert, for at de dataene som skal sendes må være beskyttet. Nøkler, ekvivalent til et privat eller personlig nummer, kan integreres i autentiserings og krypteringsfunksjoner, og intergreres i en sikkerhetprosess, som gir et resultat som er teoretisk umulig å knekke uten å kjenne nøkkelen.

  Styrken i en krypteringsnøkkel øker med lengden på nøkkelen. På grunn av restriksjoner fra enkelte lands myndigheter angående krypteringsnøkler som kan brukes ved utveksling av data utover landets grenser, bør man hvis behov for internasjonal kommunikasjon, ha tilgang til forskjellige krypteringsmetoder og nøkler med forskjellig lengde.

  Med en gang en krypteringsnøkkels lengde er valgt og implementert, er det neste skrittet å sikre at nøkkelen er beskyttet gjennom et nøkkel-håndteringssystem. Nøkkelhåndtering er prosessen hvor nøklene distribueres, oppdateres med visse intervall og tilbakekalles hvis nødvendig.

  Det er nødvendig med en balanse mellom nøkkel-utveksling intervallene og mengde av data som blir utvekslet. Et intervall som er for kort medfører overdreven prosessering for nøkkelgenerering i VPN serveren. På den annen side, for lange intervaller mellom bytte av nøkler, vil medføre at for mye data blir kryptert med den samme nøkkelen. Denne nøkkelhåndteringsprosessen må være automatisk for å beskytte nøkkelintegriteten ettersom en organisasjon vokser i kompleksitet og størrelse, vil antall nøkler øke samsvarende.

6. Forskjellige typer VPN

6.1 Remote Access VPN

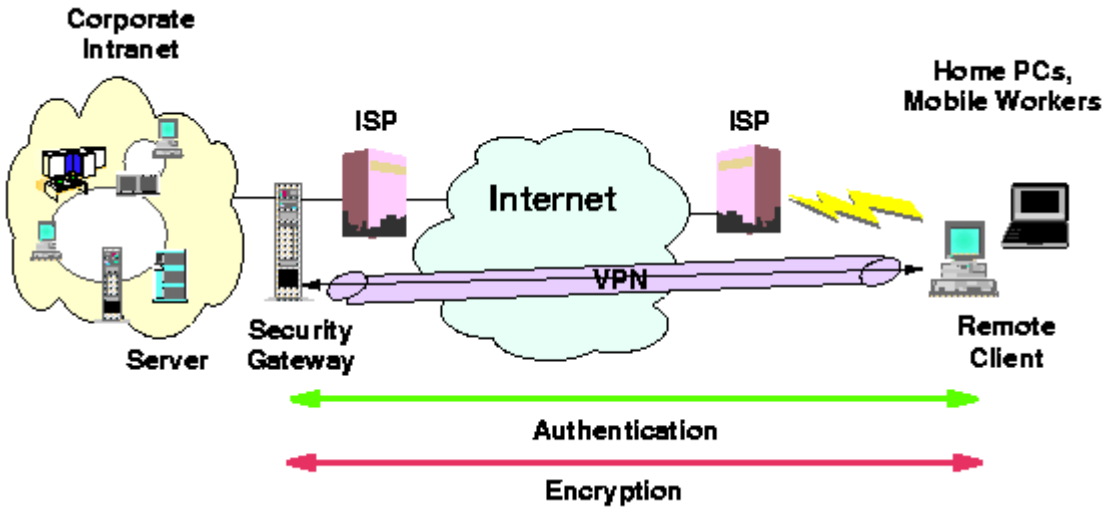
Fordelen som Internett tilbyr i forhold til vanlig oppringt forbindelse oppdages, som tidligere nevnt, av stadig flere. Mange selskaper har brukt store ressurser på store modem-pooler og penger til tellerskritt, og har i det siste funnet ut at ved å bruke Internett som det underliggende nettverket, har de muligheter til å spare penger i tillegg til at en remote-access løsning via Internett er mye enklere å implemetere, bruke og administrere.

Brukeren (client) av Remote Access VPN skal ikke behøve manuelt å starte VPN programvaren hver gang han eller hun vil starte en sikker kommunikasjonskanal . Istedenfor bør VPN programvaren startes og kjøres i bakgrunnen uten at brukeren ser den.

På serversiden er sentralisert og enkel administrasjon viktig. Overvåking av et stort antall brukere, legge til og fjerne brukere på vanlig måte, kan fort bli kaotisk og derved medføre sikkerhetsrisikoer.

I de fleste tilfeller er en bruker av remote access VPN en reisende eller en ansatt som ønkser å ha hjemmekontor. Ansatte som jobber på en slik måte ønsker å ha tilgjenglig alle ressurser og en arbeidsflate som er den samme som den de bruker når de er tilstede hos arbeidsgiver.

En typisk remote access VPN, som Figur 3 illustrerer, er når en bruker logger seg på Internett via en lokal ISP (Internett Service Provider)[i] og etablerer en kryptert tunnel mellom sin desktop og det ytre forsvarsverk til sin arbeidsgivers nettverk.



Figur 3: Remote Access VPN

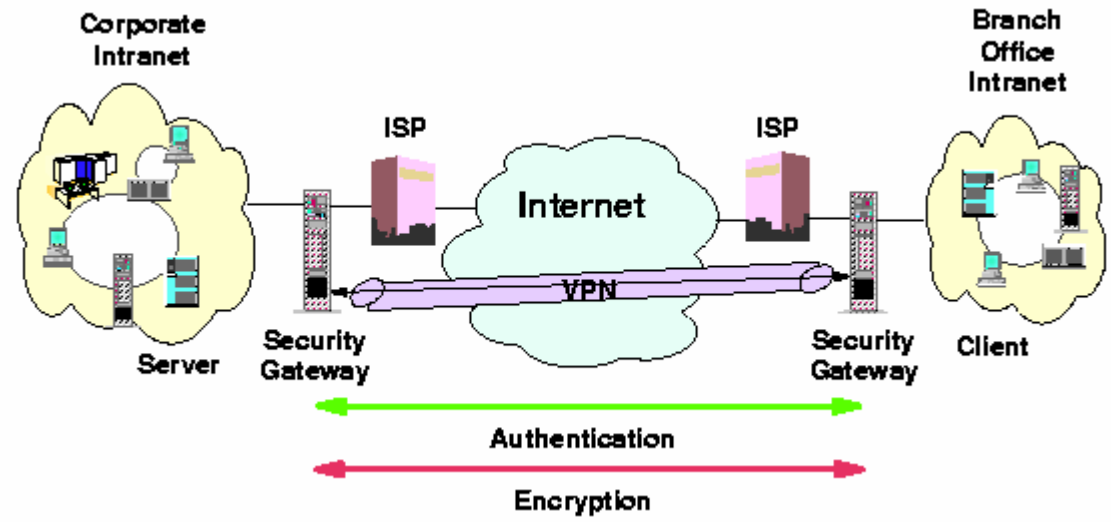
[i] ISP: Internett Service Provider: Firma som tilbyr deg tilknyttning til en Internett node, for eksempel Telenor og Tele2 her i Norge

6.2 Intranett VPN

Intranett kan beskrives som halv-permanente WAN (Wide Area Network) over et offentlig nett, og er en LAN-to-LAN forbindelse mellom to eller flere av en virksomhets lokasjoner. Som Figur 4 illustrerer blir den sikre kanalen her etablert mellom to rutere eller mellom to serverer som også kan være brannmurer, det vil igjen si mellom to sikre endepunkter.

En virksomhet som ønsker en slik løsning kan derfor konsentrere seg om styrken på krypterings og authentiserings-metodene mellom de sikre endepunktene. Det utveksles ofte store mengder med data innen et WAN (mellom to eller flere lokalnett) slik at hastighet også har stor betydning i en slik løsning.

Et sikkert intranett VPN blir karakterisert som et nett hvor bare visse brukere har tilgang, og hvor det er mulig å sette individuell tilgang for disse brukerne. I tillegg må all informasjon som sendes over det underliggende nettet være fullstendig kryptert og autentiserbart hele veien mellom endepunktene, og ikke bare mellom de forskjellige lokalnettenes ytre forsvarsverk. Slike løsninger benytter seg av protokollen IPSec som er/eller mest sannsynlig vil bli en IETF standard for IP sikkerhet, og er en del av neste generasjon IP: IPv6.

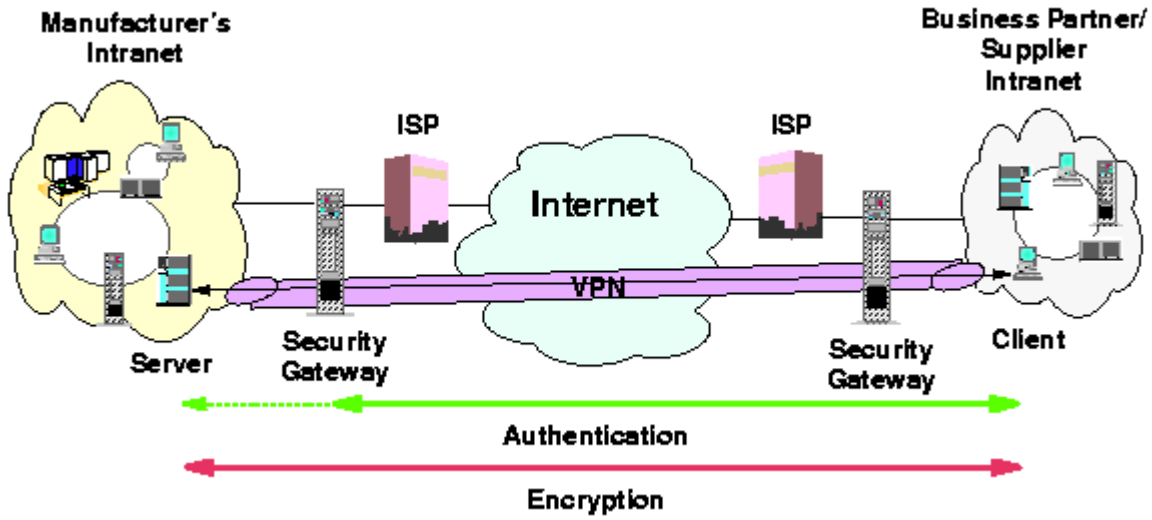


Figur 4: Intranett VPN

6.3 Ekstranett VPN

I motsetning til Intranett som brukes internt i en virksomhet, er ekstranetts formål , å nå samarbeidspartnere, kunder og leverandører, som Figur 5 illustrerer. Et ekstranett VPN må ha muligheter til å håndtere et hieraki av sikkerhet, hvor tilgang til de mest sensitive data er knyttet opp mot høyest tilgjenglige sikkerhetsmekanismer. Alle applikasjoner bør sikres, fordi de fleste samarbeidende systemer er forskjellige, og en trygg ekstranett løsning bør være allsidig med forskjellig plattformer, protokoller, autentisering og krypteringsmetoder.

Hovedmålet for et ekstranett er å sikre at konkurranse-kritiske eller sensitiv informasjon kommer riktig fram og til riktige mottaker uten å ha vært rørt av uvedkommende. Protkoller som brukes til dette formålet er IPSec, SOCKS v5[10] og SSL (SecureSocketLayer)[11].



Figur 5: Extranett VPN

7. VPN Protokoller

Oversikten som Figur 6 viser, er de forskjellige protokoller som brukes til de forskjellige formål i VPN forbindelser. Vil her komme inn på de lavere lags protokoller, SOCKs og SSL blir ikke omtalt, men taes her med som illustrasjon.

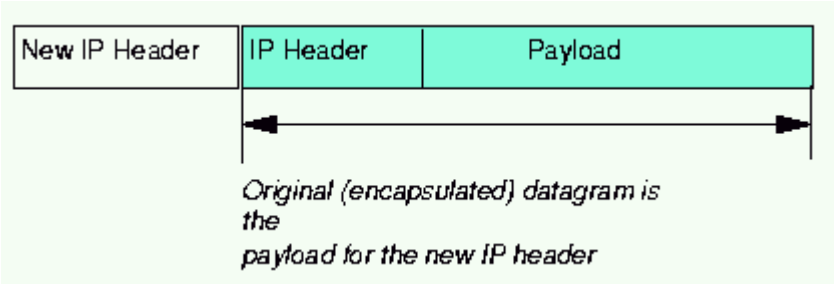
Type of VPN	OSI Layer	Technology
Trusted LAN-to-LAN	Layers 1 and 3	IPSec, Frame Relay, SMDS, etc.
Basic Remote Access	Layer 2	PPTP, L2TP
Secure Remote Access	Layer 5	SOCKS v5, SSL
Business-to-Business	Layer 5	SOCKS v5, SSL

Figur 6: VPN protokoller

7.1 Tunneling

Å transporterer informasjon effektivt og sikkert fra et punkt til et annet er tanken bak teknikken som benevnes "Tunneling". Tunneling eller innkapsling er en vanlig teknikk i pakke-svitsjede nettverk.

Som Figur 7 viser går tunneling ut på å pakke inn en pakke i en ny pakke. En ny header legges på den originale pakken, og hele den originale pakken betraktes som lasten til den nye pakken.



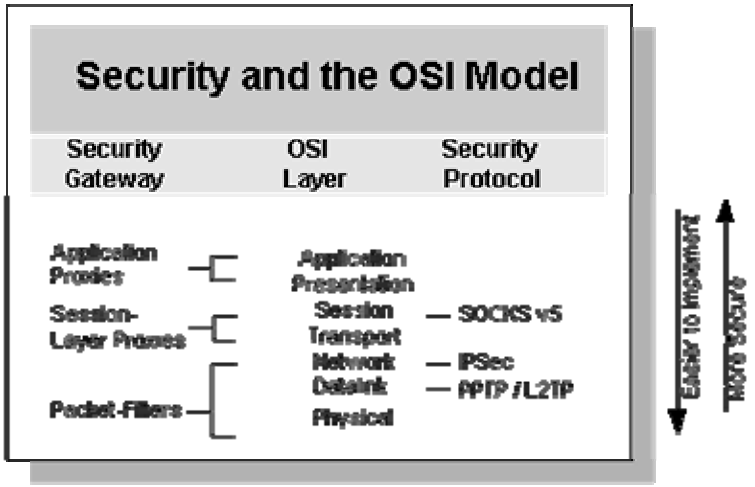
Figur 7: IP tunneling/innkapsling

Noen ganger brukes tunneling for å bære trafikk fra en protokoll over et nettverk som ikke støtter denne protokollen direkte. For eksempel, kan IPX innkapsles i IP og fraktes over et IP nett.

Protokollene som brukes for å etablere ende-til-ende kommunikasjon gjennom en tunnel over f.eks. Internett, er

- ***PPTP (Point-to-Point Tunneling Protocol)***
- ***L2TP(Layer Two Transport Protocol)***
- ***IPSec (Internet Security Protocol)***

Hvor i OSI-modellen disse protokollene opererer illustreres i figur 8, som er hentet fra hjemmesiden til Aventail [2]:



Figur 8: VPN protokoller i OSI

7.2 Tunneling Protocol (PPTP)

PPTP var en av de første tunneling protokollen som dukket opp og er basert på et forslag fra Microsoft, men utviklingen har også vært støttet av flere andre interessenter. PPTP er en tunneling protokoll som er laget for å kunne kapsle inn oppringt PPP trafikk i en sikker PPTP tunnel.
Som en tunneling protokoll, pakker PPTP [12] inn nettverks protokoll diagrammer i en IP-konvolutt. Etter at pakken er pakket inn, vil hver ruter eller maskin som møter pakken behandle denne som en IP-pakke.

Fordelen med IP innpakking er at det tillates at mange forskjellige protokoller kan rutes over et IP-nett, slik som Internett.

Istedenfor å ringe opp et modem eller ISDN ruter for å få kontakt med en privat NAS/RAS server, ringer sluttbrukeren opp en ISP og bruker PPTP for å sette opp en forbindelse til sitt privat lokalnett over Internett.

Denne oppkoblingen skjer som følgende [13]:

- **PPP tilknytning og kommunikasjon:** en PPTP klient bruker PPP for å få kontakt med en ISP ved å bruke en standard telefonlinje eller ISDN. Denne forbindelsen bruker PPP (Point-toPoint Protocol) for å etablere forbindelsen og kryptere datapakkene. Nærmere beskrivelse av PPP, se avsnitt 7.3: Point-to-Point Protocol (PPP).
- **PPTP kontroll forbindelse:** Ved å bruke forbindelsen til Internett som er etablert av PPP protokollen, lager PPTP protokollen en kontrollforbindelse fra PPTP klienten til PPTP-serveren som er tilknyttet Internett. Denne forbindelsen bruker IP for å etablere forbindelsen som kalles PPTP tunnel.
- **PPTP data tunneling:** Tilslutt, lager PPTP protokollen IP datagram som inneholder krypterte PPP pakker som blir sent via PPTP tunnelen til PPTP serveren. PPTP serveren pakker ut IP datagrammene og dekrypterer PPP pakkene, og ruter videre de dekrypterte pakkene til det private nettverket.

Figur 9 er hentet fra Mirosofts hjemmesider [13] og illustrerer hvordan PPTP protokollen spesifiserer en serie av kontrollmeldinger som sendes mellom PPTP-klienten og PPTP-serveren. Kontrollmeldingene etablerer, vedlikeholder og avslutter PPTP tunnelen.

Kontrollmeldingene blir sendt som kontrollpakker i et IP-datagram. En IP-forbindelse blir opprettet mellom PPTP-klienten og PPTP-serveren. Denne kontroll forbindelsen brukes for å utveksle kontrollmeldinger, og kontrollmeldingene er detaljert beskrevet i Internett draftet Point-to-Point Tunneling Protocol (PPTP).

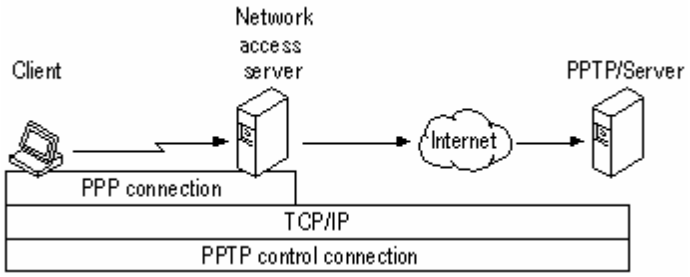
Meldings type	Formål
PPTP_START_SESSION_REQUEST	Starts Session
PPTP_START_SESSION_REPLY	Replies to start session request
PPTP_ECHO_REQUEST	Maintains session
PPTP_ECHO_REPLY	Replies to maintain session request
PPTP_WAN_ERROR_NOTIFY	Reports an error on the PPP connection
PPTP_SET_LINK_INFO	Configures the connection between client and PPTP Server
PPTP_STOP_SESSION_REQUEST	Ends session
PPTP_STOP_SESSION_REPLY	Replies to end session request

Figur 9: PPTP kontrollmeldings typer

Som Figur 10 viser består IP-datagrammet, som inneholder kontrollmeldingen, av en PPP header, en IP header, en PPTP kontroll-melding og en egnet trailer (en hale):

Figur 10: PPTP kontroll melding

Figur 11 viser hvordan utvekslingen av meldinger mellom PPTP-klienten og PPTP-serveren skjer over IP forbindelsen.Disse meldingene blir brukt til å etablere og vedlikeholde en PPTP-tunnelen.



Figur 11: PPTP kontroll forbindelse

Når forbindelsen er opprettet starter dataoverføringsfasen:

- **PPTP Data Transmisjon:**
  PPTP bruker en forsterket Generic Routing Encapsulation (GRE)[i] mekanisme for å støtte flyt- og opphopningskontoll ved transport av de innkapslede PPP-pakkene. Denne forsterkningen medfører at tunnelen som brukes til transport av brukerdata blir støttet med lavnivå opphopningskontroll og flytkontroll. Denne mekanismen medfører en effektiv bruk av båndbredden som er tilgjengelig for tunnelen og hindrer unødvendig retransmisjon og at bufferne overlastes. PPTP dikterer ikke hvilke algoritmer som skal brukes til disse lavnivå kontrollene, men definerer hvilke parametre som må utveksles for å få disse algoritmene til å virke.
- **Sikkerhet i PPTP:**
  Sikkerheten for brukerdata som passerer gjennom tunnelen for PPP forbindelsen, er PPPs oppgave, og er også autentisert av PPP endene (peer). Siden PPTPs kontrollkanal ikke hverken er autentisert eller integritetssikret, så kan det være mulig for en angriper å få tilgang til den underliggende IP forbindelsen. Det er også mulig å skape falske kontroll-kanal-meldinger og endre ekte meldinger under transport uten at det blir oppdaget.
- **Autentisering:**
  Autentiseringen av en remote PPTP klient skjer ved å bruke PPPs autentiserings metode når klient ringer opp til nettverks aksess serveren. Hvis PPTP serveren er tilknyttningen til ditt private nettverk , vil denne kontrollere tilgangen til dette. Hvis en Windows NT server er konfigurert som en PPTP server, krever den derved standard Windows-NT basert logon, det vil si med brukernavn og passord. PPTP servere under andre OS har samme

[i] Generic Routing Encapsulation (GRE): en tunneling protokol som brukes for å innkapsle PPP datapakker i en IP pakke, utviklet av Cisco.

tilgangsrutiner. Man bør derfor ha en streng passord policy, med passord som innholder en minimums antall tegn og som er vanskelig å gjette.

- **Aksess kontroll:**
  Aksess kontrollen avhenger av hvilket nettverksoperativsystem som er på det private nettverket og tilgangen til ressursene derunder avhenger av begrensninger som er satt på brukernivå.
- **Kryptering av data:**
  PPTP bruker PPPs kryptering og PPPs komprimerings metode.

7.3 Point-to-Point Protocol (PPP)

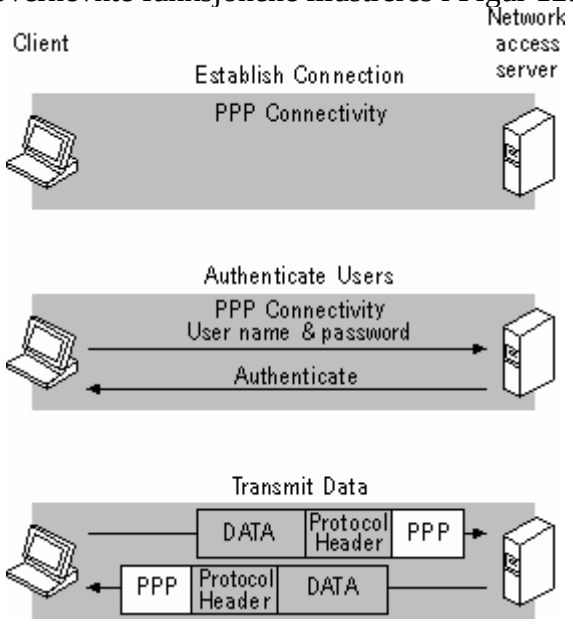
PPP [14] er en internett standard for innkapsling av multi-protokoll datagram for transport over en point-to-point link, det vil her si oppringte samband.

PPP protokollen brukes av PPTP for å sende multi-protokolldata over et IP basert nettverk.

PPP pakker inn IP, IPX og NetBEUI pakker i PPP rammer og sender de innpakkede pakkene ved å lage en point-to-point link mellom klienten og nettverkets aksess-server og støtter følgende funksjoner:

- **Etablerer og terminerer den fysiske forbindelsen**
- **Autentifiserer brukere**
- **Lager PPP datagram**.

Disse overnevnte funksjonene illustreres i Figur 12:



Figur 12: PPP forbindelse

PPP beskriver også en Link Control Protocol (LCP) som er ansvarlig for etablering, konfigurering og vedlikehold av forbindelsen. PPP Encryption Control Protocol (ECP) [15] er ansvarlig for konfigurering og åpning av krypteringsalgoritmene som skal brukes.
En kryptert pakke blir innkapslet i en PPP informasjons fil, hvor PPP protokoll feltet indikerer at typen er en kryptert datagram (hex0053). Den vanligste krypteringsmetoden som PPP bruker er Data Encryption Standard (DES), også kalt PPP DES encryption protocol [16].

Kompresjon kan også brukes i tillegg til kryptering og skjer ved å bruke Compression Control Protocol [17]. Klar tekst må først komprimeres og etterpå krypteres som resulterer mindre data og en sikrere kryptering.

I noen løsninger, hvor en klient/bærebar PC med nettverkskort kan bruke en Internett tilknyttning i f.eks. et konferanserom, vil den direkte IP forbindelse medføre at den initielle PPP forbindelsen er unødvendig. Klienten kan initiere en PPTP forbindelse direkte til PPTP serveren uten å etablere en PPP forbindelse til ISP først.

7.4 Layer 2 Tunneling Protocol (L2TP)

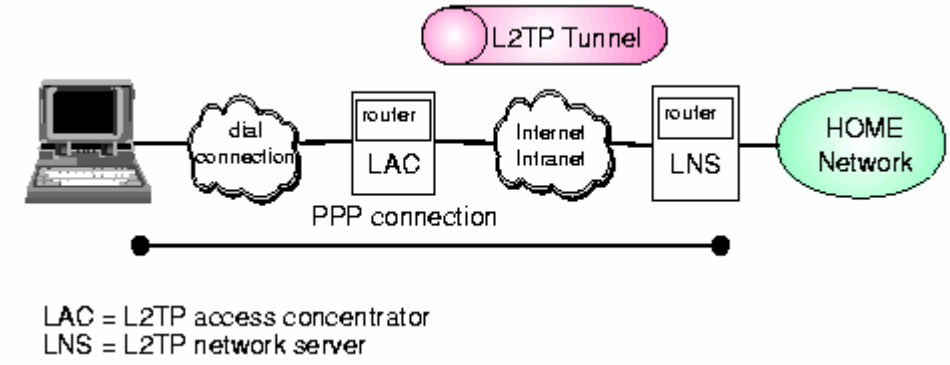
Mens Microsoft arbeidet med PPTP, utviklet Cisco Systems[18] en protokoll som de kalte Layer 2 Forwarding (L2F).

L2F protokollen hadde omtrent samme funksjonaliteten som PPTP, men med en vesentlig forskjell i og med at tunneling funksjonen var plassert i ruter hardwaren. L2F krever derfor rutere som støtter L2F i begge endene av kommunikasjonskanalen.

L2TP er en IEFT standard som kombinerer de beste egenskapene til L2F og PPTP. L2TP er en utvidelse av PPP, og sikkerheten ivaretas av PPP, som f.eks. autentisering av brukerne.

Tradisjonelt har oppringte nettverkstjenester bare støttet registrerte IP adresser som igjen har begrenset typer av applikasjoner som kunne implementeres over VPN. L2TP støtter multiple protokoller og uregistrerte og private IP adresser over Internett. L2TP som PPTP, muliggjør at tunnelen initieres av klienten eller av en nettverks aksess server.

I L2TPs Internet draft [19] defineres en tunnel som en forbindelse mellom en L2TP Network Server (LNS) og en L2TP Access Consentrator (LAC), som vist på Figur 13.



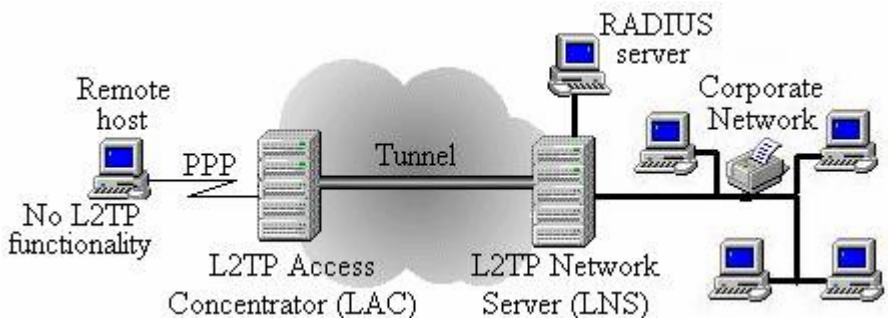
Figur 13: L2TP tunnel

Tunnelen bærer PPP datagram mellom LAC'n og LNS'n, og mange sesjoner kan multiplekses innen en enkel tunnel. En kontrollforbindelse operer over den samme tunnel. Denne kontrollforbindelsen kontrollerer etableringen, vedlikeholdet og administrasjon av sesjonene og selve tunnelen.

Ved bruk av L2TP som tunneling protokoll i et Remote Access VPN skjer tilgangen til det private nettet med PPP fra et asynkron modem eller synkron via ISDN.

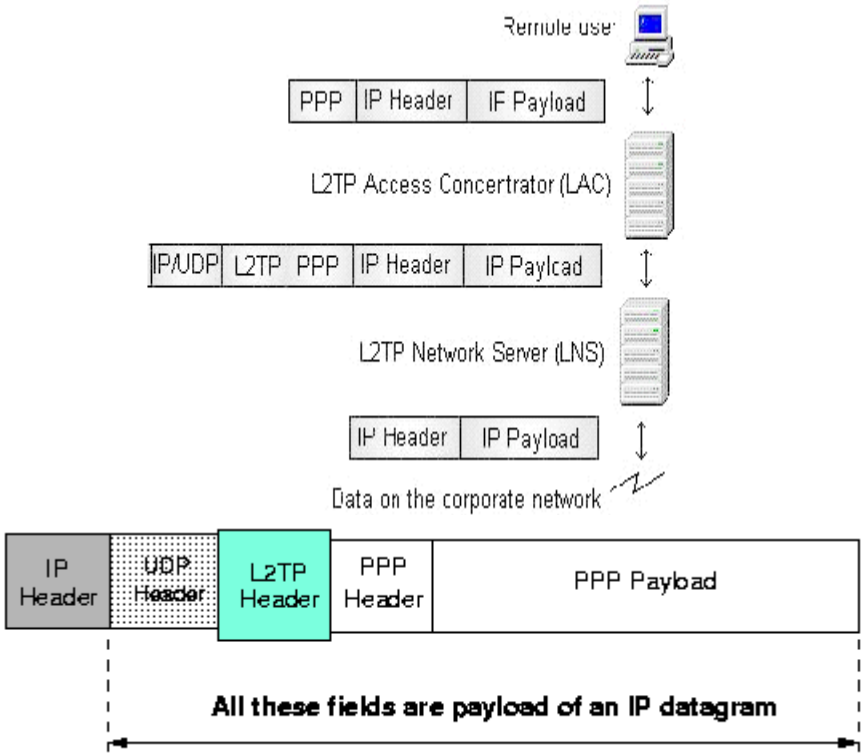
Figur 14 viser hvordan forbindelsen settes opp fra en remote klient som ikke støtter LT2P.

I dette tilfellet vil den oppringte forbindelsen skje mot en L2TP Access Consentrator (LAC) som drives av en ISP. LAC er en Network Access Server (NAS) eller en host samlokalisert med et PPP endesystem, som har muligheten til å håndtere L2TP protokollen. LAC'n setter opp forbindelsen til det private nettets L2TP Network Server (LNS).



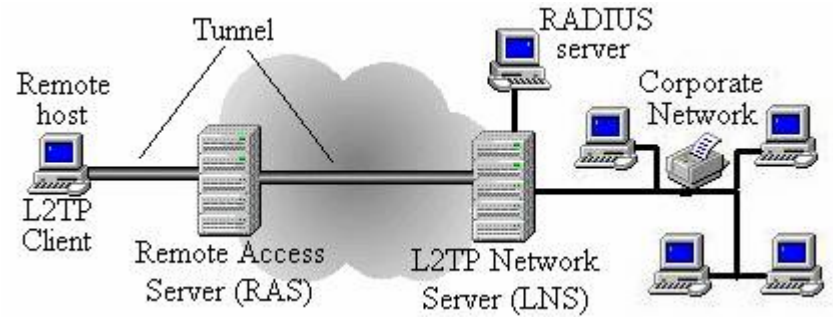
Figur 14: "ikke-L2TP" klient mot nettverk som bruker LAC, LNS og RADIUS-server

En "ikke-L2TP-klient" sender PPP pakker til L2TP Access Consentratoren (LAC), som innkapsler disse innkommende pakken i L2TP pakker og pakken transporteres gjennom tunnelen til L2TP Network Serveren. LNS fjerner innkapslingen på L2TP pakkene og sender dem videre inn i det private nettverket, som illustrert i Figur 15.



Figur 15: Innkapsling ved L2TP

Hvis klienten støtter L2TP, illustrerer Figur 16 hvordan denne setter opp en tunnel via Remote Access Server (RAS)/Network Access Serveren (NAS), gjennom Internett, og avslutter tunnelen i LNS på det private nettverket.



Figur 16: L2TP-klient mot nettverk som bruker Network Access Server/Remote Access Server, LNS og RADIUS

Som figurene viser er hovedforskjellen ved kommunikasjon fra en "ikke-L2TP-klient" og klient som støtter L2TP, er start og ende punktet for tunnelen. For en "ikke-L2TP-klient" starter tunnelen først når man har nådd NAS serveren på ISP nettverket, men begge tunnelene avsluttes hos LNS.

Et L2TP nettverk kan også inkluderer en "Remote Authentication Dial-in User Service" (RADIUS) server [20].

RADIUS serverens oppgave i et L2TP nettverk kan blant annet være å stå for autentisering av brukeren og tildeling IP adresse. RADIUS serveren sentraliserer autentiseringsfunksjonen og fjerner nødvendigheten for å konfigurere hver LNS med brukernavn og passord. RADIUS tildeler også IP-adresser til remote maskiner slik at disse kan identifiseres som en del av det private nettverket.

7.5 Frivillig eller tvungen tunneling ved PPTP og L2TP

For å konstruere et VPN som Remote Access VPN snakkes det om skille mellom *klient initiert tunneling* og *NAS initiert tunneling*. Den førstnevnte refereres ofte til som "voluntary" (frivillig) tunneling, mens den siste vanligvis betegnes som "compulsory" (tvungen) tunneling.

- **Frivillig tunneling**

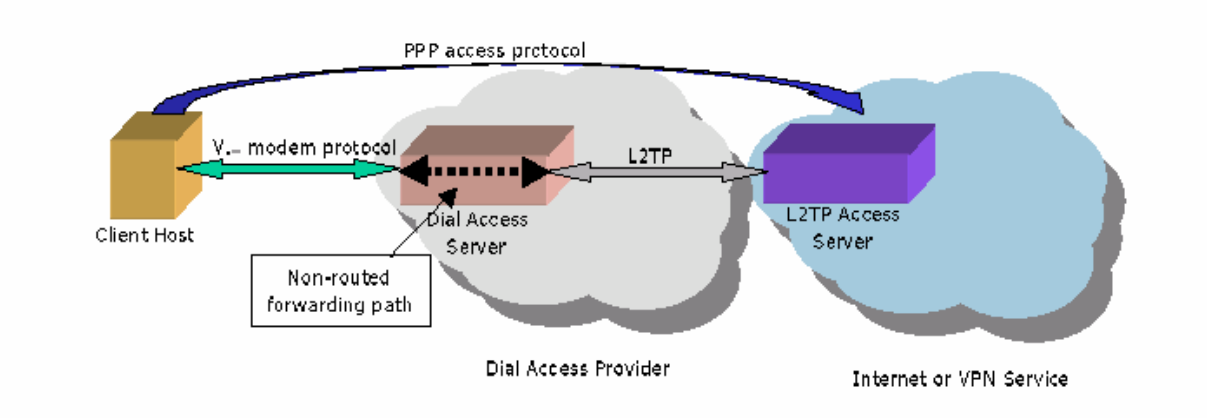
Frivillig tunneling er når tunnnelen etableres etter forespørsel fra brukeren til et spesifikt formål.

- **Tvungen tunneling**

Tvungen tunneling er når tunnelen opprettes automatisk sett fra brukerens side, og uten at brukeren har noe valg eller ser at dette skjer.

L2TP, som en tvungen (compulsory) tunneling modell, er i all vesentlighet en mekanisme for å henge opp en oppringt bruker til et annet punkt i nettverket, eller til et annet nettverk .

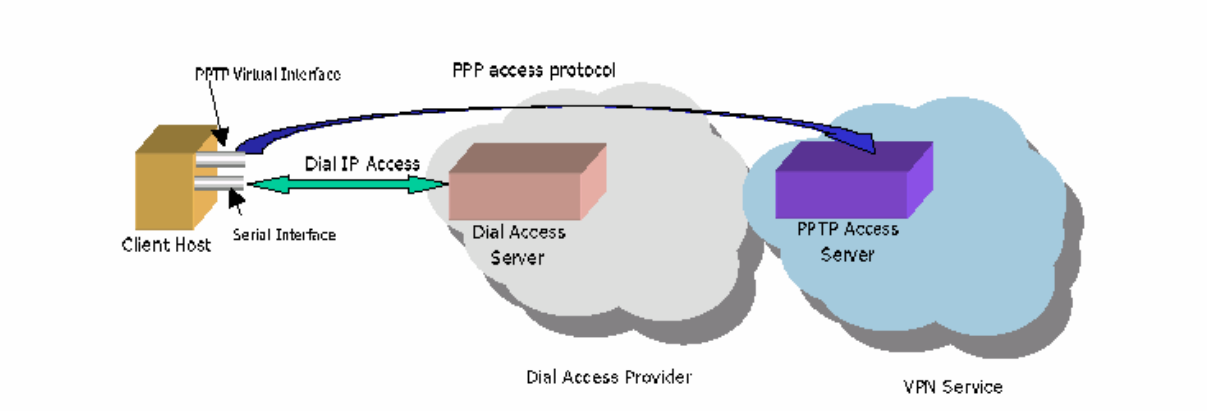
Figur 17 illustrerer en tvungen tunneling situasjon . Brukeren ringer opp en NAS (i figuren Dial Access server) og brukeren autentiseres basert på en lokal konfigurert profil. L2TP tunnel blir dynamisk opprettet til det (utfra konfigurasjon på brukeren) *forhåndsdefinerte endepunktet*, hvor brukerens PPP sesjon avsluttes.



Figur 17: Remote VPN L2TP klient

På den annen side beskrives PPTP som en frivillig (voluntary) tunneling modell, se Figur 18. Da er det endesystemene (f.eks. en desktop) som konfigurere og etablere individuelle adskilte ende-til-ende tunneler til vilkårlige lokaliserte PPTP servere, uten at en mellomliggende NAS trenger å være involvert i PPTP avslutningen eller tunnel etableringen.

Som illustrert i Figur 18, ringer klienten til en NAS (i figuren Dial Access server), og PPP sesjonen avsluttes i NAS som i en tradisjonell PPP modell. Den påfølgende PPTP sesjonen opprettes, mellom klient endesystemet og en vilkårlig klientvalgt PPTP server. PPTP serveren nåes via tradisjonell ruting informasjon hvis brukeren har blitt tildelt privilegier på PPTP serveren.



Figur 18: Remote Access VPN PPTP klient

Med PPTP og frivillig tunneling, har den brukeren på en oppringt forbindelse mulighet til å velge PPTP tunnelens endepunkt etter at PPP initieringen er avsluttet. Dette er viktig, hvis

tunnel endepunktene som brukeren ønsker å aksessere skifter til stadighet. Det blir da ikke nødvendig å forandre i mellomleddene fra den remote brukeren.

Det er også betydelig nytte i at PPTP tunneler er transparente for ISP'n, og at ingen avansert konfigurasjon trenges mellom NAS operatøren og det overliggende oppringte tilgangen til VPN.

I et slikt tilfelle, har ikke ISP'n PPTP serveren, men bare enkelt lar PPTP trafikken passere på samme måte som vanlig som normal IP trafikk.

Ved L2TP med en tvungen tunneling implementasjon, kontrollerer ISP hvor PPP sesjon avsluttes. Dette kan være veldig viktig i en situasjon hvor ISP, som brukeren ringer inn til, må sette PPP sesjonen opp via et annet nettverk enn vanlig.

I L2TP draftet beskrives ikke i detalj alle mulige implementasjoner eller anvendelses områder for protokoll. Den grunnleggende anvendelsestilfellet er kort beskrevet sammenlignget med resten av dokumentet, og er muligens ensidig konsentrert mot en "compulsory" tunneling modell. Ikke desto mindre finnes det implementasjoner av L2TP som følger "voluntary" modellen. Det finnes også forskjellige implementasjoner av L2TP klienter som anvender frivillig tunneling.

Om PPTP eller L2TP er mest formålstjenelig ved anvendelse av VPN avhenger av om man ønsker at kontrollen må ligge hos ISP eller hos klienten. Forskjellen kan karakteriseres utfra klienten i et VPN, hvor L2TP modellen er en tjeneste hos en "grossist" som har et antall av konfigurerte klient tjenestetilbud, som kan være VPN i et vanlig oppringt aksess system. Mens PPTP modellen er *en* av distribuerte private aksesser hvor klienten er en individuell sluttbruker og VPN strukturen er en ende-til-ende tunnel.

Forskjellen kan også sees i økonomiske sammenhenger, i og med at L2TP modellen tillater en tjenestetilbyder å tilby en verdiskapende tjeneste utenom vanlig IP tjenester, og takstserer sine brukere etter hva de vil bruke og derved få nye inntekter, mens PPTP modellen åpner for en distribuert tilgang til VPN og lar sammarbeidende VPN utvide aksess mulighetene uten nødvendigheten av særskilte service kontrakter med forskjellige ISP'er.

8. Internet Protocol Security (IPSec)[21]

Internett Protocol Security (IPSec) er en IEFT standard for IP sikkerhet. IPSec er designet for å støtte høy kvalitets krypterings-basert sikkerhet til anvendelse både for IPv4 og IPv6.

Samlingen av sikkerhetstjenester som støttes inkluderer accesskontroll, forbindelsesløs intergritet (helhet), data opprinnelses autentisering, beskyttelse mot gjentakelse (en form for partiell (delvis) rekkefølge integritet), konfidensialitet (kryptering) og begrenset trafikk flyt konfidensialitet.

Data opprinnelses autentisering verifiserer at hvert datagram virkelig ble sendt av den som utgir seg over å være senderen. Data intergritet verifiserer at hvert datagram ikke blir forandret under overføringen, enten bevisst eller på grunn av feil.

Data konfidensialtet betyr at klarteksten i en melding skjules ved kryptering, og gjentakelses-beskyttelse sikrer at en angriper ikke kan snappe opp et datagram eller spille det tilbake (gjenopprette) på et senere tidspunkt.

Disse tjenestene tilbys på IP laget, og gir beskyttelse for IP og/eller overliggende protokoller (om f.eks TCP, UDP, ICMP etc.) og blir gjennomført ved bruk av to trafikk sikkerhets protokoller; Authentication Header (AH) og Encapsulating Security Payload (ESP) og videre gjennom bruk av krypteringsnøkler, vedlikeholdsprosedyrer og protokoller.

Måten samlingen av IPSec protokoller blir benyttet , og til hvilket formål de er iverksatt, vil avdekkes av hvilke sikkerhet- og systemkrav brukerne, appliksjonene og organisasjonen har.

8.1 Hva gjør IPSec ?

IPSec tilbyr sikkerhetstjernester på IP laget ved å la et system velge ønskede sikkerhets-protokoller, bestemme hvilke algoritmer som skal brukes for tjenestene, og bruke hvilken som helst kryteringsnøkkel for å tilfredstille de ønskede tjenestene.

IPSec kan brukes for å beskytte en eller flere "veier" mellom to hosts, mellom to sikkerhets-"port"-maskiner (gateway) eller mellom en host og en gateway. En ruter eller en brannmur som er implementert med IPSec kalles en sikkerhets-gateway.

8.2 Hvordan virker IPSec

IPSec bruker som nevnt to trafikk sikkerhets protokoller;

- **Authentication Header** (AH)[22] og
- **Encapsulating Security Payload** (ESP)[23].

IP Authentication Header (AH) tilbyr forbindelsesløs integritet, data opprinnelses autentisering og en valgfri anti-replay tjeneste

Encapsulating Security Payload (ESP) kan tilby konfidensialitet (krypetring), og begrenset trafikk mengde konfidensialitet. Den kan også tilby forbindelsesløs integritet, data opprinnelses autentisering og anti-replay tjeneste. En eller flere av disse tjenestene må anvendes uansett når ESP er iverksatt.

Både AH og ESP er et redskap for access kontroll, basert på distribusjon av krypteringsnøkler og styringen av trafikk flyten som er relatert til disse sikkerhetsprotokollene.

AH og ESP protokollene kan anvendes alene eller i kombinasjon med hverandre for å tilby et bestemt sett av sikkerhetstjenester i IPv4 og IPv6. Begge protokollene kan brukes på to måter: i transport modus eller i tunnel modus.

I transport modus tilbyr protokollene beskyttelse primært for de overliggende lags protokoller og i tunnel modus anvendes protokollene for å overføre IP pakker gjennom en tunnel.

8.3 Authentication Header (AH)

Som nevnt brukes Authentication Header (AH) for å gi forbindelsesløs integritet, data opprinnelses autentisering av IP datagram, og en valgfri anti-replay tjeneste.

Tjenester i AH

Data integriteten sikres av en sjekksum som generes ved bruk av en "message authentication function", f.eks. MD5 [24] + [25],

data opprinnelses autentisering sikres ved å inkludere en delt sikkerhetsnøkkel i dataene som skal autentiseres, for eksempel v.h.a. Hashing Authentication Code (HMAC) [26], og

anti-replay tjenesten implemteres ved å bruke et sekvens-nummer felt i AH-headeren.

HMAC-MD5 [27]

Målet for HMAC-MD5 er å sikre at pakken er ekte og ikke blir modifisert under transport. HMAC er en sikkerhets-nøkkel autentifikasjons algoritme. Data integritet og data original autentifikasjon som blir sørget for av HMAC og er avhengig av omfanget på utdelingen av sikkerhetsnøkler. Hvis bare avsender og mottaker kjenner HMAC nøkkelen, gir det både autentifikasjon av dataenes originalitet og data integritet for pakker sendt mellom disse to partene. Hvis HMAC er riktig beviser dette at den må være lagt til av adressaten

Hva gjør AH ?

De overnevnte tjenestene er forbindelsesløs, det vil si at de arbeider på pr-pakke basis.
AH autentiserer så mye av IP datagrammet som mulig. AH beskytter hele innholdet i et IP datagram unntatt visse felt i IP headeren (kalt mutable fields). Disse feltene vil normalt bli modifisert mens IP datagrammet rutes gjennom nettverket.
De skiftende feltene i IPv4 er:

- Type of Service (TOS)
- Flags, Fragment Offset
- Time to Live (TTL) og
- Header Checksum.

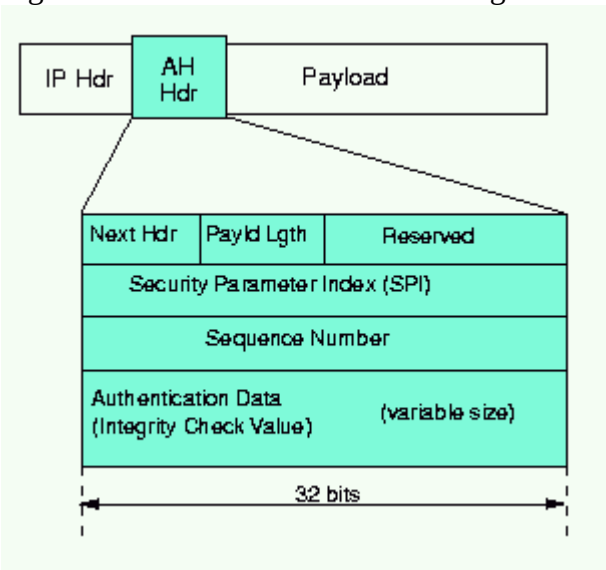
Når det kreves at disse feltene skal beskyttes, må tunneling brukes. Lasten i IP pakkene kan betraktes som uforanderlige og er alltid beskyttet av AH. Ved kalkulasjon for integritetsjekk-verdi, vil de feltene som kan forandres behandles som om de ikke inneholder noe. Integritetssjekk-verdien er en del av AH-headeren. AH er identifisert ved protokoll nummer 51.

AH behandling kjøres bare på ikke-fragmenterte IP pakker. En IP pakke med AH kan fragmenteres av mellomliggende rutere, og i så tilfelle vil mottaker først reassemble pakken og etterpå starte AH prosesseringen på den. Hvis en IP pakke som viser seg å være fragmentert (offset-feltet er forskjellig fra 0, eller at flere-fragment-bitet er satt), og er inndataene til en AH behandling, vil den bli kastet. Dette hindrer et såkalt overlapping frament angrep, som misbruker fragment-reassembling algoritmen for å lage forfalskede pakker og få de igjennom brannmurer.

Pakker som feiler ved autentifikasjon blir kastet og aldri levert til det overliggende laget. Denne måten å operere på reduserer betraktelig sjangsene for et heldig "denial of service" angrep, som har til formål å blokkere kommunikasjon for en maskin eller en gateway ved å overflomme den med falske pakker.

8.3.1 AH Header Format

Figur 19 viser hvor AH headeren er lagt i en IP pakke og hvilke felter AH består av:



Figur 19: AH header format

Feltene i Authentication Header'n:

- ***Next Header:***
  Next Header er et 8-bitsfelt som identifiserer hvilken type data som kommer etter AH. Denne verdien er valgt fra listen over IP standard protokollnummer som finnes i "Assigned Numbers" RFC" [28] fra the Internet Assigned Numbers Authority (IANA) [29].
- ***Payload Length:***
  Dette feltet er også 8-bit langt og viser lengden til selve AH headeren uttrykt i 32-bits ord, minus 2. Det relaters ikke til den aktuelle payloaden eller lasten i IP pakken som helhet. Hvis default verdien er brukt, er verdien 4 (tre faste 32 bits ord pluss tre 32 bits ord med autentiseringsdata minus 2)
- ***Reserved:***
  Dette feltet er reservert for framtidig bruk. Det har en lengde på 16 bit og er satt til 0.
- ***Security Parameter Index (SPI):***
  Dette feltet er 32 bit langt. Se Security Parameter Index avsnitt 9.1.1.
- ***Sequence Number:***
  Dette 32bits feltet er en voksende teller som blir brukt for replay-beskyttelse. Replay-beskyttelse er valgfri, men dette feltet er påbudt. Senderen inkluderer alltid dette feltet og det er opptil mottakeren å behandle det eller ikke. Sekvensnummer kan ikke repeteres og dette feltet henger nøye ilag med bruken inneholdet i Security Association (SA), se avsnitt 9.1.1.
  Anti-replay er altså default i bruk hos senderen. Hvis SA hos mottakeren ikke er valgt å bruke anti-replay, så bryr ikke senderen seg mer om verdien i dette feltet. Notér likevel at anti-replay mekanismen brukes ikke ved manuell nøkkelhåndtering.
- ***Authentication Data:***
  Dette feltet er av variabel lengde og kalles også Intergrity Check Value (ICV).

ICV for en pakke blir kalkulert ved hjelp av en forhåndsbestemt algoritme. Authentication Data feltets lengde er udelt sammensatt av 32 biter. Som navnet tilsier blir det brukt av mottaker for å verifisere integriteten av innkommende pakker.
I teorien kan uansett MAC algoritme brukes for å kalkulerer ICV. Spesifikasjon krever at HMAC-MD5-96 og HMAC-SHA-1-96 må støttes, men i praksis blir også Keyed-SHA-1 brukt. Vanligvis støtter implementasjoner to til 4 algoritmer. Når ICV kalkulasjon skjer blir de feltene som kan endres satt til 0.

8.3.2 Authentication Header (AH) i transport og tunnel modus

Opprinnelig IP datagram:
Figur 20 illustrerer et originalt IP-datagram, slik det sendes uten noen form for sikkerhet:

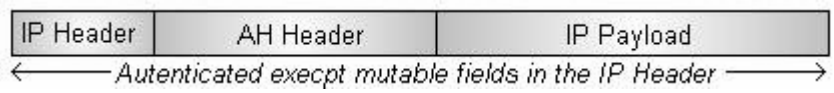
Figur 20: Normalt IP datagram

AH kan enten anvendes i transport- eller tunnel modus. Det medfører at det originale IP datagrammet, innkapsles på følgende måte:

AH i Transport modus:
I transportmodus, er den originale IP headeren den ytterste IP headeren, slik som vist på Figur 21.

IP headeren følges av en AH-header, og etter det kommer lasten/informasjonen fra det originale IP datagrammet.

Det originale IP datagrammet, så vel som AH-headeren, er autentisert, og uansett forandring i noe felt, se bort fra de før nevnte som forandres under transport, kan detekteres. All informasjon i datagrammet er i klartekst, og er derfor mulig å avlytte under overføring.



Figur 21: Datagram ved bruk av AH i transport modus

AH i Tunnel Modus:
I tunnel modus, blir en ny IP header generert for bruk som den ytterste IP header i det nye datagrammet.

Sender og mottakeradresse i den nye IP headeren vil vanligvis være forskjellig fra den originale sender og mottakeradressen.

Den nye header følges av en AH-header, og videre av det originale IP datagrammet, hvor både headeren og lasta er som den opprinnelige.
Hele det nye datagrammet, som vist på Figur 22, er beskyttet av AH protokollen. Forandring i noe felt i et tunnel modus datagram kan detekteres. All informasjon er klartekstform.

Figur 22: Datagram ved bruk av AH i tunnel modus

AH kan brukes alene, i kombinasjon med ESP eller til og med innkapsles i enn annen form av seg selv. Med disse kombinasjonene, autentisering kan leveres mellom et par kommuniserende parter; mellom to hoster, to brannmurer eller mellom host og brannmur.

8.4 Encapsulating Security Payload (ESP)

Tjenester i ESP:
ESP brukes for å støtte:

- integritets sjekk
- autentifikasjon og
- kryptering av IP datagram.
- Valgfri replay beskyttelse er også tilstede.

Disse tjenestene er forbindelsesløse, det vil si at de opererer pr. pakke og ikke alle er tvungen brukt.

Men en kommer ikke utenom følgende: integritetssjekk og autentifiksjon arbeider i lag.

Replay beskyttelsen er valgfri bare med integritet og autentisering og kan bare velges av mottaker.

Kryptering er valgfri, men er avhengig av de andre tjenestene. Det anbefales sterkt at hvis kryptering er i bruk, så må integritetssjekk og autentisering også brukes. Hvis bare kryptering brukes, kan inntrengere plassere falske pakker i sendingen med det formål å knekke krypteringen. Dette er umulig hvis også intergritets sjekk og autentisering brukes.

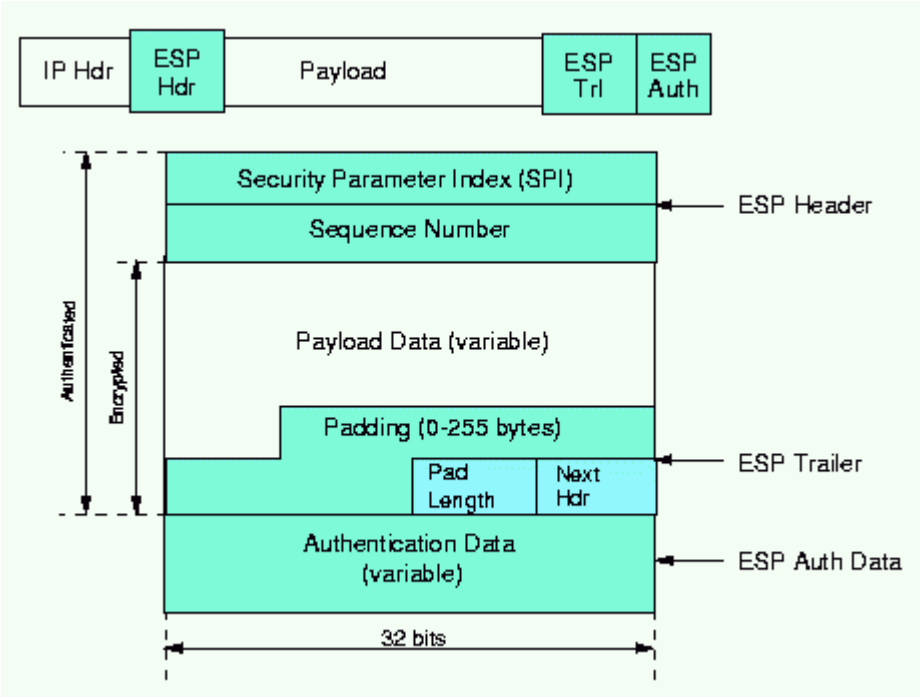
Til tross for at både autentisering (med integritetssjekk) og kryptering er valgfritt, så er alltid minst en av dem valgt. Ellers er det i realiteten ikke noen vits å bruke ESP i det hele tatt.

ESP identifiseres ved protokollnummer 50. ESP behandling kan bare brukes på ikke-fragmenterte IP pakker. En IP pakke med ESP kan fragmenteres i mellomværende rutere. I så tilfelle reassemblerer mottakeren først pakkene, før de blir ESP prosessert. IP pakker som er fragmentert og blir forsøkt ESP behandlet, blir kastet.

Hvis både kryptereing og autentisering med intergritetssjekk blir valgt, så vil mottakeren først autentisere pakken, og bare hvis det var vellykket forsettes det med dekryptering. Denne måten å jobbe på sparer prosseserings ressurser og reduserer sårbarheten ved angrep.

8.4.1 ESP Packet Format

Formatet til en ESP pakke, som vist i Figur 23, er mer komplisert enn en AH pakke. Det har ikke bare en ESP header, men også en ESP trailer (hale) og ESP autentiseringsdata. Den innkapslede lasten er mellom headeren og traileren, i henhold til protokollens navn.



Figur 23: ESP pakke format

Feltene ved bruk av ESP:
Som Figur 23 viser, er de følgende felt deler i en ESP pakke:

- ***Security Parameter Index (SPI):***
  32 bits felt for å identifisere Security Associations for forbindelsen. Se 9.1.1.

- ***Sequence Number:***
  32-bits felt som inneholder en teller. Se videre forklaring i 8.3.1.

- ***Payload Data:***
  Payload feltet er påbudt. Det består av et variende antall bytes med data som beskrives i NextHeader feltet. Dette feltet er kryptert med den krypteringsalgoritmen som er valgt ved SA etableringen. Hvis algoritmenn krever initieringsindikatorer, så er disse også inkludert her. ESP spesifikasjon krever støtte for DES algoritmen i CBC modus (DES-CBC transform)[30].

- ***Padding:*** De fleste krypteringsalgoritmer krever at data som skal behandles av algoritmen er i hele antall blokker. Altså, som resultat må cipherteksten (inkludert Padding, PadLength og NextHeader) må avsluttes på en 4-bytes grense, slik at NextHeader-feltet kommer kant-i-kant (eller rett etter). Dette er årsaken til at dette feltet av variabel lengde er tatt med. Det kan også brukes til å skjule lengden av den originale meldingen. Imidlertid kan dette ha en negativ innvirkning på effektiv båndbredde. Padding er et påbudt felt. Krypteringen beskytter PayLoad Data, Padding, PadLenght og NextHeader feltene.

- ***Pad Length:*** Dette er et 8-bits felt som består av antall foregående padding bytes (stuff-bytes). Det er tilstedeværende, og hvis verdien er 0 indikerer det at det ikke er noe padding.

- ***Next Header:*** NextHeader er et 8-bits påbudt felt som viser hvilken datatype som lasten består av, f.eks. en høyere lags indetifikator slik som TCP. Verdi er valgt fra IP Protocol Numbers definert av IANA.

- ***Authentication Data:*** Dette feltet varierer i lengde og inneholder ***Integrity Check Value (ICV).*** Integrity Check Value'n kalkuleres for ESP pakken *fra SPI feltet til og med NextHeader feltet*.
  Authentication Data feltet er valgfritt. Det inkluderes bare når integritets sjekk og autentisering er valgt i SA (se side 30) ved initialisering. ESP spesifikasjonene krever støtte for to autentiseringsalgoritmer: HMAC med MD5 og HMAC med SHA-1[31]. Noter at IP headeren ikke beskyttes av ICV.

8.4.2 Encapsulating Security Payload (ESP) i transport og tunnel modus

ESP kan også brukes i transport- eller tunnel modus, og medfører som for AH, at det originale IP datagrammet innkapsles på følgende måte:

Figur 24: Normalt IP datagram

ESP i Transport modus:
I transport modus vil ESP's autentiseringsfunksjoner bare beskytte det originale IP lasten, men ikke den originale IP headeren.

Figur 25 illustrerer ESP i transport modus, hvor bare datagrammets originale IP header beholdes.

Bare lasten fra det originale datagrammet og ESP traileren blir kryptert. IP headeren er ikke hverken autentisert eller kryptert. Dette medfører at en angriper har tilgang til både sender og mottakeradresse mens pakken transporteres.

Figur 25: Datagram ved bruk av ESP i transport modus

ESP i Tunnel modus:
I tunnel modus, se Figur 26, vil ESP autentiseringen beskytte den originale IP headeren og IP lasten, men ikke den nye IP headeren.

Figur 26: Datagram ved bruk av ESP i tunnel modus

I tunnel modus blir en ny IP header generert. Hele det originale IP datagrammet (både header og last) og ESP traileren blir kryptert.

Fordi den originale IP headeren er kryptert, vil den ikke være synlig for en eventuell angriper. Derfor brukes ESP vanligvis i tunnel modus for å skjule intern adresseinformasjon mens pakken transporteres og derved hindre uvedkommende å gjennomføre f.eks. trafikkanalyser.

ESP brukes på samme måte som AH. på den måten at den kan anvendes alene, i kombinasjon med AH eller nøstet inn i seg selv.

8.5 Transport eller tunnel modus

Som nevnt kan både AH og ESP brukes både i transport og tunnel modus.

IPSec tunnel modus er en innkapslingsteknikk som er lagt etter "IP Encapsulation within IP"[32] utfra følgende punkter:

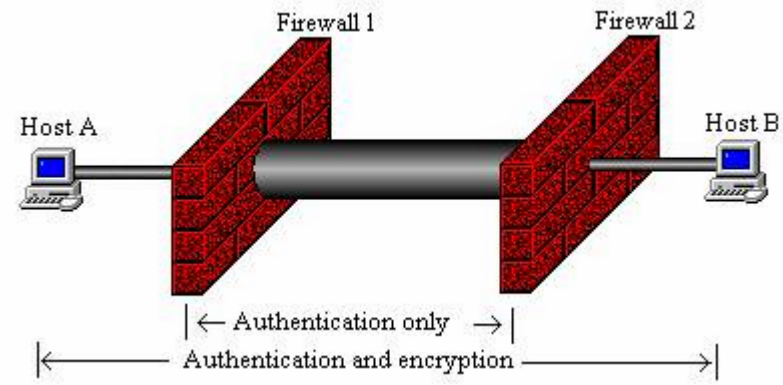
- ***Transport modus:***
  anvendes normalt mellom to endepunkt i en forbindelse. F.eks. hvis sikker kommunikasjon er oppfyllt langs alle involverte elementer på veien fra klient til server, så bruker klient og serveren IPSec i transport modus.
- ***Tunnel modus:***
  brukes normalt mellom to maskiner hvor minst den ene av dem ikke er et endepunkt i forbindelsen.
  For eksempel: hvis sikker kommunikasjon er oppfylt melom to brannmurer som står mellom en klient og en server, vil brannmurene bruke tunnel modus mellom seg.

  Eller hvis en remote maskin ringer inn til sitt lokalnett ønsker den å ha en sikker kommunikasjonsvei mellom seg og inngangsmaskinen til sitt lokalnet. Det vil igjen si at klienten og gatewayen på klientens private lokalnett anvender IPSec i tunnel modus i en slik situasjon.

8.6 Gjentagende innkapsling

Mens transporten mellom to brannmurer foregår, transporteres det originale datagrammet innkapslet og oversendes som last i et nytt datagram med en ny header. En slik innkapsling kan i teorien brukes gjentagende, og føre til en innkapsling som består av mange nivåer. I praksis støtter IPSec bare to nivåer av innkapsling.

Figuren [33] under viser hvordan slik innkapsling skjer i flere nivåer:



Host A bruker ESP i transport modus

Brannmur 1 bruker AH i tunnel modus

Brannmur nummer 2 mottar AH tunnel datagrammet og gjenoppretter det originale datagrammet som brukte ESP i transport modus, og dette gjennomrettede datagrammet videresendes til host B.

9. Internet Security Associations Key Management Protocol (ISAKMP)[34]

9.1.1 Security Association(SA)

Konseptet med Security Associations (SA) er fundamentalt for IPSec. SA inneholder informasjon om hvilke sikkerhetstjenester som skal brukes for en gitt forbindelse. Benevnelsen Security Association er et konsept, og kan implemeteres på uttalige måter. SA konseptet brukes både av AH og ESP, en av hovedfunksjonene for IKE (Internet Key Exchange)[35] er å etablere og vedlikeholde SA'ene.
En SA er en unidirectional (simpleks/enveis) logisk forbindelse mellom to IPSec systemer, som entydig identifiseres med følgende tre parameter:

<Security Parameter Index, IP Destination Address, Security Protocol>:

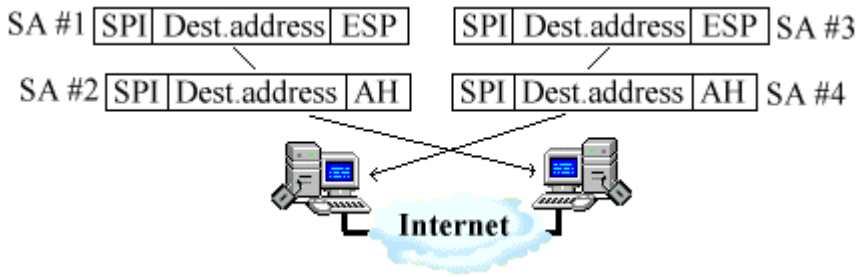
- ***Security Parameter Index (SPI):***
  Dette er en 32-bits verdi som brukes for å identifiserer forskjellige SA'er som har den samme destinasjons- adresse og sikkerhetsprotokoll.
  SPI er med i headeren på sikkerhetsprotokollen (AH eller ESP). SPI har bare lokal betydnig, som definert av den som har laget SA'et.

SPI kan ikke ha en verdi mellom 1 og 255 siden disse er reservert av Internet Assigned Numbers Authority (IANA). SPI verdien 0 må bare brukes for lokal implemtasjonsspesifike formål.
Vanligvis velges SPI av destinasjons systemet når SA etableres.

- ***IP Destination Address:***
  Adressen kan være en unicast, broadcast eller en multicast adresse.
  SA vedlikeholds mekanismer er imidlertid ikke bare definert for unicast adresser.
- ***Security Protocol:*** kan enten være AH eller ESP eller begge

Et SA kan brukes i en av to moduser: transport eller tunnel, avhengig av modusen til protokollen som er valgt i denne SA.

Fordi SA's er enveis, for toveis kommuikasjon mellom to IPSec system, må det være to SA'er definert, en i hver retning.
Et enkelt SA kan ikke tilby både AH sikkerhet og ESP sikkerhet som medfører at dette må gjøres ved å bruke Multiple SA. Dette betyr at to hoster som kommuniserer og bruker både AH og ESP må bruke 4 SAs, en for hver sikkerhetstjeneste, to i hver retning, slik Figur 27 illustrerer.



Figur 27: Fire SA brukt mellom 2 hoster

Et SA leverer sikkerhetstjenester til trafikk som bæres ved bruk av enten AH eller ESP, men ikke begge.

Med andre ord: For at en forbindelse som skal beskyttes av både AH og ESP, må to SA'er defineres i hver retning.

I et slikt tilfelle, vil settet av SA'er som definerer forbindelsen bli referert til som en *SA bunt*. SA'ene i en bunt må ikke termineres i samme endepunkt. For eksempel, en mobil maskin kan bruke en AH SA mellom seg selv og en brannmur og en nestet ESP SA som strekker seg til en maskin bak brannmuren.

En IPSec implementasjon administrerer ***to databaser*** som er relatert til SA'ene:

- ***Security Policy Database (SPD):***
  Sikkerhets ***styrings***-databasen spesifiserere hvilke sikkerhetstjenester som kan tilbys til IP trafikken, avhengig av faktorer som kilde, destinasjon, om det er inngående eller utgående trafikk etc.

  Den inneholder bestemet liste av styrings oppslag, forskjellige for innkommende og utgående trafikk. Disse oppslagene kan spesifisere at noe trafikk ikke skal gjennomgå IPSec prossesering, at noe skal avvises/fjernes og at resten skal prosesseres av IPSec modulen.

Oppslag i denne databasen kan sammenlignes med brannmur regler eller pakkefiltere.

- ***Security Association Database (SAD) :***
  Sikkerhets ***tilknytnings***-databasen inneholder parameter informasjon for hvert SA, slik som AH eller ESP algoritmer og nøkler, sekvensnummer, protokoll modus og hvor lenge SA'et skal gjelde.

  For utgående prosessering, vil et oppslag i SPD peke på et oppslag i SAD. Det som skjer da er at SPD'n finner ut hvilken SA som skal brukes for en gitt pakke.

  For inngående trafikk blir SAD konsultert for å finne ut hvordan den innkommende pakken skal behandles.

9.1.2 The Internet Key Exchange (IKE) Protocol

Som nevnt, Security Association (SA) inneholder all relevant informasjon som kommunikasjonsystemet trenger for å kjøre IPSec protokollene, som AH og ESP. Et SA vil identifisere krypteringsalgoritmen som skal brukes, nøkkelinformasjon, identifisere deltalkerne etc.

ISAKMP definerer et standard rammeverk som skal støtte av formidlingen av Security Association (SA), initiere genereringen av alle krypteringsnøkler, og følgende oppdatering/fornyelse av disse nøklene.

Oakley er en påbudt administrasjonsprotokoll som kreves brukt innenfor ISAKMPs rammeverk. ISAKMP støtter automatisk formidling av Security Association (SA) og automatisk generering og fornying av krypteringsnøkler.

Muligheten til å håndtere disse funksjonene med liten eller ingen manuell konfigurasjon av maskinene vil være kritiske element for et VPN som vokser i størrelse. Sikker utveksling av nøkler er det mest kritiske faktoren ved etableringen av et sikkert kommunikasjon-miljø, uansett hvor sterk autentiseringen og krypteringen er, så vil de bli verdiløs hvis nøkkelen avsløres.

Siden ISAKMP prosedyrene avtales ved initieringen av nøklene, må de være i stand til å bli kjørt over linker hvor det antas at det ikke eksisterer noen sikkerhet. Det er, de brukes for å starte (laste opp) IPSec protokollene. Som følge av det, bruker ISAKMP protokollene de mest komplekse og prossessor-intensiver operasjonene i IPSec protokoll settet.

ISAKMP krever at all informasjonsutveksling må være både kryptertert og autentisert. Ingen kan avlytte nøkkel materiale, og nøkkel materiale vil utveksles bare mellom autentiserte deltakere.

9.1.3 SAKMP/Oakley Oversikt

ISAKMP metodene er designet med det klare mål for å beskytte mot forskjellige vel kjente risikoer, som eksempel:

- **Denial-of-Service:** meldinger konstrueres med unike cookies som kan bruks for å raskt identifiserer og forkaste ugyldige meldinger uten å bruke prosessor-intensive krypterings operasjoner.
- **Man-in-the-Middle:** Det er ønskelig med beskyttelse mot vanlige angrep som fjerning av meldinger, modifikasjon av meldinger, sending av meldinger tilbake til sender, replay av gamle meldinger og forandring av retning til meldinger til mottakere som ikke var ment å motta meldingen.
- **Perfect Forward Security (PFS):** Avsløringen av forgangne nøkler krever ikke mange ledetråder for å knekke andre nøkler, enten det skjer før eller etter den avslørte nøkkelen. Det medfører at hver nøkkel som er fornyet må utvinnes uten noen tilknyttning til de foregående nøklene.

9.1.4 To faser ved ISAKMP/Oakley

Hvor robust en krypteringbasert løsning er avhenger mer av hvor strengt en holder nøklene hemmelig, enn de faktiskedetaljer til de valgte krypteringsalgoritmene. På grunn av det har IEFT IPSec Working Group foreskrevet et sett av robuste ISAKMP/Oakley utvekslings protokoller.

Det brukes en to-fase tilnærming:

- ***Fase 1:***
  For å beskytte brukerdata trafikken, foretaes det først forhandlinger/avtaler om å etablerer en overordnet "hemmelighet" som alle krypteringsnøklene etterhvert utledes fra.

  Vanligvis brukes offentlig nøkkel kryptografi for å etablere en ISAKMP Security Association (SA) mellom systemene, og for å etablere nøkler som vil bli brukt til å beskytte de ISAKMP meldingene som skal kjøres når forhandlingene i den etterfølgende *Fase 2* foregår.

  Fase1 har bare betydning under etablereingen av sikrings-settet for selve ISAKMP meldingene, men den etablerer ikke noen "security associations" eller nøkler for å beskytte brukerdata.

  I *Fase 1* er krypteringsoperasjonene de mest prosessor-intensive, men er ikke nødvendig å utføre så ofte. I tillegg kan *en* enkelt *Fase 1* utveksling brukes for å støtte flere påfølgende *Fase 2* utvekslinger.

  Som en tommelfinger regel: operasjon for å gjøre *Fase 1* forhandlingene utføres en gang for dagen eller kanskje en gang i uken, mens *Fase 2* forhandlinger utføres med få minutters mellomrom.

- ***Fase 2:***
  Fase 2 forhandlingene er mindre komplekse, siden de bare brukes etter at avtalte sikkerhetstilpassninger fra *Fase 1* er aktivisert.

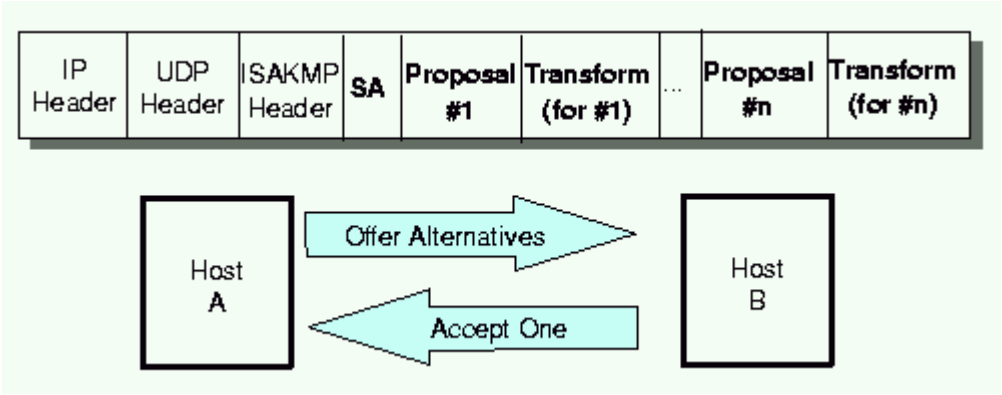
Et sett av kommunikasjonssystemers forhandler om "security associations" og nøkler som skal beskytte utvekslingen av brukerdata.

Fase2 ISAKMP meldinger blir beskyttet av de ISAKMP "security associations" som ble generert i *Fase1*. Forhandlinger opptrer vanligvis oftere i *Fase2* enn *Fase 1*. For eksempel, en typiskk applikasjon som bruker Fase2 avtalen må oppdatere krypteringsnøklene hvert andre eller tredje minutt.

ISAKMP protokollen tilbyr også en løsning når den remote maskins IP adresse ikke er kjent på forhånd. ISAKMP tillater en remote maskin å identifisere seg selv med en permanent identifikator, slik som et navn eller en e-mail adresse.

ISAKMP *Fase1* utvekslingen vil da autentisere den remote maskins permanent identitet ved å bruke offentlig nøkkel kryptografi:

- Sertifikater lager en binding mellom den permanente identifikatoren og en offentlig nøkkel. Derfor kan ISAKMPs sertifikat-baserte *Fase 1* meldingsutveksling autentisere den remote maskinens permanente identifikator.
- Siden ISAKMP meldingene selv bæres inni et IP datagram, kan ISAKMP partnere (f.eks. en brannmur eller en destinasjons maskin) forbinde den remote maskins dynamiske IP adresse med dens autentiserte permanente identifikator.



Figur 28: Meldingsutveksling (negonations/forhandlingsstart)

Figur 28 viser meldingsutveksling i en *Fase 1* forhandling. Maskin A er den initerende part, som vil konstruere en ISAKMP melding i klartekst og sende denne til Maskin B. Selve ISAKMP meldingen sendes som last i en UDP pakke, som igjen bæres som last i et normalt IP datagram.

Videre vil maskin A og B fortsette forhandlingene om hvilke sikkerhets parametre som skal brukes i henhold til beskrivelsen om *Fase 1* og *Fase 2*.

10. VPN Produkter

Det finnes uttalige leverandører av produkter som benevnes som VPN løsninger. Jeg har imidlertid valgt å gå gjennom to produkter som er basert på hardware-kryptering: RedCreek Communications Ravlin 10[36] og Shiva Corporations LanRover VPN Gateway[37].

10.1 RedCreek Communications Ravlin

Generelt:
RedCreek's Ravelin Hardware VPN systemer er:

- Ravelin 4
- Ravelin 10
- Ravelin 100

og

- Ravlin 45/PCI adapter kort.

Disse enhetene bruker alle den samme CryptoCore™ arkitektur og IP nettverkslags sikkerhets standard. RedCreeks Ravlin er nettverks-sikkerhetsløsning som yter kryptering og dekryptering med en "troughput" opp mot Ethernets maksimum hastighet

Det betyr at hardware krypto-boksene klarer opp til 100 Mb/sek (Ravelin 100). Dette gir en reell "on-the-fly" kryptering og dekryptering..

Ravlin bruker:

- 40 bit/56 bit DES og 168 bits Triple DES kryptering [i]
- Autentisering og access kontroll støttes ved bruk DSS (Digital Signature Standard) [38]
- Diffie-Hellman nøkkel-utveksling [39]
- X.509 v.3. digital sertifikat [40]
- ISAKMP/Oakley nøkkel håndtering**Error! Bookmark not defined.**.

Som nevnt før er disse sikkerhet-standardene en del av IETF's IPSEC standard.

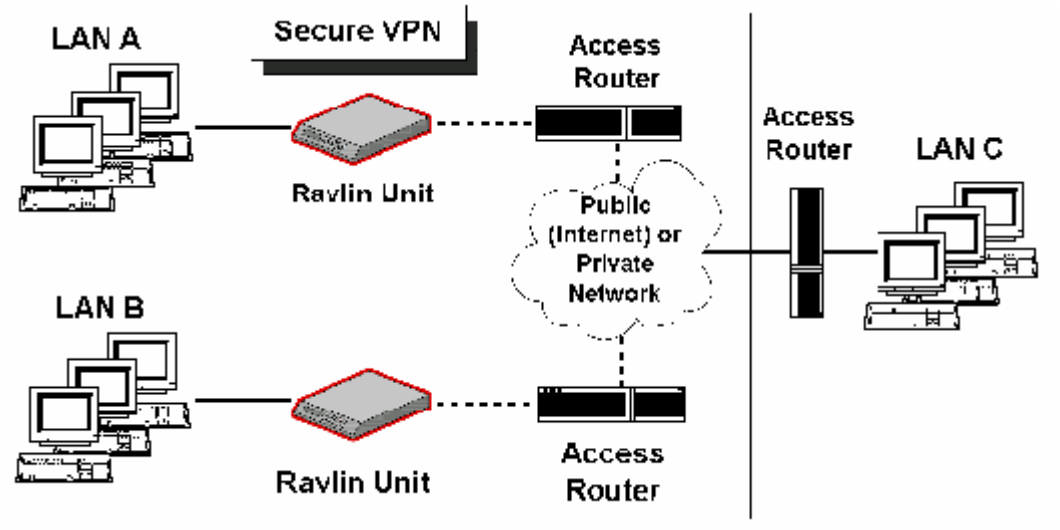
Ravlin hardware boksene jobber mot RavlinSoft Client som kjøres under Windows 95, Windows NT 4.0 og Windows for worksgroups 3.11. RedCreeks Ravlin støtter RADIUS (RFC 2138 kompatible) for autentisering.

En fullstendig VPN løsning fra RedCreek, som vist i Figur 29, er i tillegg til selve Ravlin boksen, programvare for:

- klient **RavlinSoftClient**

[i] Triple DES: Særskilt blokk-krypteringsmetode som er bygget på DES som brukes tre ganger med to forskjellige nøkler: Meldingen krypteres først på vanlig måte med en nøkkel. Deretter dekrypteres meldingen denne chifferteksten med en ny nøkkel, noe som gir en ny chiffertekst. Til slutt krypteres denne siste chifferteksten med den første nøkkelen.

- administrasjon **RavlinNodeManager** .



Figur 29: VPN med Ravlin fra RedCreek

I de fleste tilfellene brukes Ravlin-boksen for å beskytte kommunikasjon mellom to LAN over et offentlig nett.

Ravlin boksen installeres typisk mellom lokalnettet og access-ruteren for dette lokalnettet, som vist i Figur 29. Lokalnett A og B er sikre nett, men lokalnett C er ikke en del av dette sikre nettet.

Ravlin boksene beskytter her kommunikasjon (IP-pakker) som utveksles mellom Lokalnett A og Lokalnett B, mens kommunikasjon til/fra Lokalnett C er ubeskyttet. Beskyttelsen som Ravlin boksen yter, er den sikkerheten som er definert i Security Associations for den aktuelle sesjonen.

10.1.1 Encrypt-in-place (EIP)

I tillegg til IPSec bruker Ravlin en RedCreek propietær protokoll kalt Encrypt-in-Place (EIP). Protokollen er et tillegg som brukes istedenfor ESP.

I EIP-mode vil bare lasten i IP-datagrammet krypteres. Som i ESP mode, bruker EIP mode 40-bit/56-bit DES eller 168-bit Triple DES, og kombinerer høy hastighet på alle krypteringsnivåer. EIP opererer bare i transport modus, og krypterer lasten uten å bygge om pakken med å legge til nye headere.

10.1.2 RedCreeks Ravlin 10

Ravlin 10 er kjent som en stand-alone-enhet som sørger for nettverk og sikkerhets tjenester, inkludert kryptering. Ravlin 10 krypterer data ved 10 Mbps (full duplex). En Ravlin 10 enhet

har to interface, lokal interface og remote interface, hvor det ene interfacet utveksler IP-pakker fra det beskyttede nettverket og det andre mot det eksterne nettet.

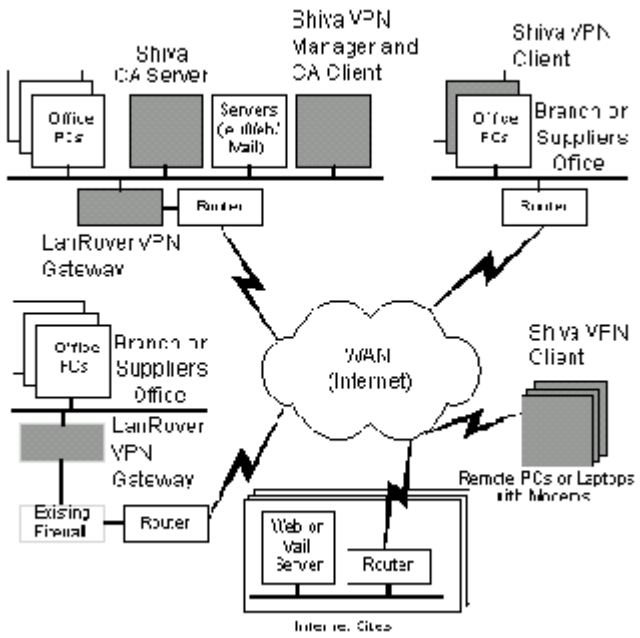
Hver enhet har altså to interface med hver sin hardware-adresse og vil derved ha forskjellige IP-adresser. Ravlin 10 kan enten kjøres som ruter eller bru. Når Ravlin 10 kjøres i bru-modus, kan den kommunisere mot bare ett annet nettverk, og i ruter-modus, mot flere nett samtidig.

10.2 Shivas LanRover VPN konsept

Generelt:
Shivas VPN løsning består av fire moduler som virker ilag for å betjene en sikker kommuniksasjon over ett hvert nettverk. Disse modulene er

- LanRover VPN Gateway™
- Shivas VPN Manager™
- Shivas VPN Client™
- Shivas Certificate Authority™[41]

En fullstendig VPN løsning fra Shivas inneholder alle modulene som illustrert i Figur 30:



Figur 30: VPN fra Shiva med LanRover VPN Gateway

LanRover Gateway'n er et hardware/software sikkerhets system som har ansvar for å prosessere datapakker som passerer mellom et offentlig og et privat nett. VPN Gateway er laget for å håndtere tre funksjoner. På kommunikasjonsnivået skal VPN Gateway virke enten som en ruter eller en bro. Den skal i tillegg kryptere pakker, og VPN gateway'n kan selektivt

kryptere/dekryptere data basert på kilde eller destinasjons adresse og porter. Det siste gir fleksibilitet m.h.p. at det kan sendes både data i klartekst og kryptert versjon over samme infrastruktur. Som brannmur, kan VPN Gateway brukes som et pakkefilter og som en proxy inspektør.

VPN Manager er en Windows 95 eller Windows NT programvarepakke for sentral monitorering og konfigurering av VPN Gateway'en. I tillegg brukes VPN Manager for å adminstrere VPN Client brukere og gi disse ønskede rettigheter og tjenester.

VPN Client er en Windows 95 eller Windows NT basert programvarepakke som gir sikkerhet mellom client-maskinen og VPN Gateway'n innenfor det private nettverket eller over WAN. Siden alle Shivas produktene opererer på nettverkslaget, er VPN Clienten usynlig for brukeren og jobber mot alle applikasjoner. Med VPN Clienten kan brukerne ringe opp til hvilken som helst ISP og lage en sikker kanal til det private nettverket.

LanRover VPN gateway boksen inkluderer et industristandard PCI bus kort som øker hastigheten på kryptering/dekrypteringen tilpasset lokalnettets hastighet. Dette kortet inkorperer en dedikert ASIC chip som er optimalisert for DES og Triple DES kryptering og sørger for betydelig økning i "throughput'n" i forhold til kryptering som bare er basert på programvare.

Shivas LanRoverVPN produkter er designet for å vokse med en organisasjons nettverk, og nye VPN uniter kan legges til etter behov, til for eksempel en typisk nettverkskonfigurasjon som vist på Figur 30.

10.2.1 Shiva Smart Tunneling (SST)

Shivas bruker foruten ESP en egen protokoll kalt SST Encapsulation. SST blir brukt for utveksling av data mellom Shivas VPN komponenter. SST sies å være betydelig sterkere enn ESP encapsulation. ESP brukes bare ved kommunikasjon mot ikke-Shivas produkter. Shivas VPN Gateways produktene bruker ESP bare i tunnel modus, og transport modus som bare krypterer lasten støttes ikke.

Når innpakkingen settes til SST må følgende informasjon spesifiseres for få definert en sikkerhets profil fullt ut:

Autentifikasjonsmetode: denne må settes til enten sertifikat, "challenge phrases", SecurID eller RADIUS. Challenge phrases (anropsfrasen/setningen/uttrykket) blir ofte referert til som autentifikasjonsnøkler, som SA vil bruke for å autentisere enheten når den første forespørselen for autentisering kommer fra enheten. Den samme anropsfrasen skal også være lagt inn i enheten før den første forespøresel skal gjøres. Noen ganger kalles "challenge phrases" for passord, men det er ikke noe godt synonym.

Public key length: Lengden på den offentlige nøkkelen må settes til 512/1024/2048 bits. Som nevnt brukes offentlig nøkkel ved autentisering og nøkkelutveksling.

Crypto period length: Krypteringsperioden definerer hvor lenge en hemmelig nøkkel kan brukes. Default verdien er en måned, men kan også settes så lavt som 3 timer.

10.2.2 Shivas LanRover VPN Gateway

Landrover VPN Gateway er hjørnestein i Shivas omfattende VPN løsning. LanRover VPN Gateway kan brukes på eksisterende oppringt samband og leide-linje løsninger for å gjøre overgangen til neste generasjons VPN teknologi enkel.

Hensikten med LanRover VPN Gateway er å spare kostnader ved å gå bort fra oppringte samband med dyre tellerskritt , leide linjer og frame-relay forbindelser, og istedenfor rute organisasjonens trafikkbehov over Internett gjennom fullstendig private forbindelser, tunneler.

LanRover VPN Gateway gir muligheter til å velge sikkerhetsnivå på tunnel-til-tunnel basis, og LanRover VPN Gateway støtter et stort valg av sikkerhetsteknologier som kontrollert tilgang og data integritet, skalerbarhet og hemmeligholdelse.

I tillegg kan det velges X.509 digitale sertifikater, RADIUS, Securty Dynamics, Entrust eller Windows NT Domains autentifikasjons system. Alle sensitive data blir beskyttet i private tunneler med standard og triple-DES kryptering. LanRover VPN Gateway sies å være lett å implementere og funksjonene er transparente for sluttbrukerne.

Shivas VPN Manager gir sentralisert administrasjon fra hvilken som helst Windows95/NT system.

Å ta i bruk alle fordeler ved LanRover VPN Gateway går ikke på akkord med nettverkets ytelse. LanRover VPN Gateway delene er basert på rask Pentium teknologi, dedikerte ASIC krypteringsteknologi og en real-time multitasking kjerne for å gi en unik kombinasjon av sikkerhet og ytelse. Hardware-basert krypteringsmulighetene skal gi styrken som kreves for å sikre samsvarende yteevne.

11. Sammenligning av to VPN produkter

På Internett ser man tydelig at utviklingen pågår hele tiden innen VPN produkter. Stadig nye leverandører lanserer nye produkter, forbedringer og nye fasiliteter. Et søk etter VPN relaterte linker ga et overkommelig resultat i januar i år, mens i dag (mai 1999) må man spesifisere sine søk ganske nøyaktig for i det hele tatt å se ”skogen for bare trær.”

For å illustrere, vil jeg som eksempel sitere fra Internett Week (April 12, 1999)[42] :
”Et potensielt problem ved å bruke et VPN internt er ytelse. Hvis data passerer i Ethernett hastighet mellom en server og en arbeidsstasjon, kan det skje at arbeidsstasjonens CPU muligens ikke klarer å takle kryptering og tunneling oppgavene i en slik hastighet.

Et par leverandører har tatt tak i dette ”on-network VPN” ytelses spørsmålet. For eksempel, sist måned introduserte RedCreek Communication Inc. ”The Personal Ravlin”, en enkelt bruker hardware VPN IPSec klient. Denne "lommeformat" enheten er utviklet for å takle krypterings- og tunneling-oppgaver for en fjernbruker når denne bruker høyhastighets kabel eller digitale abonnent linje tjenester.”

Til tross for den raske utviklingen har jeg forsøkt å sammenligne Redcreeks Ravlin 10 og Shivas LanRover VPN Gateway. Ut fra de tilgjengelige spesifikasjoner for produktene har jeg satt opp en tabell over detaljene på neste side. Gjør igjen oppmerksom på at dette er produkter

som hele tiden er under utvikling, og at disse spesifikasjonene allerede kan være ”ute av dato”, og helt oppdaterte detaljer må hentes hos leverandør eller produsent.

Sammenligningstabell VPN		
• ***Leverandør:***	RedCreek Communication Inc. Ravlin10	Shiva Corporations LanRover VPN Gateway.
• ***Nettadresse***	Www.redcreek.com	www.shiva.com
• ***Prosessor***	32-RISC Inter i960RD	Pentium
• ***Brannmur***	Nei	Ja, ICSA-sertifisert [43] Circuit-Level Firewall
• ***Trafikk modus***	Bru/ruter	Bru/Ruter
• ***Ruting protocol***	Proxy Arp	Static Routing
• ***VPN Protocol***	IPSec AH/ESP	IPSec AH/ESP
• ***Propietære protokoller***	EIP (encrypt-in-place) (se avsn.10.1.1)	SST (shivas-smart-tunneling) (se 10.2.1)
• ***LAN interface***	10Base-T	10BASE-T/100BASE-T
• ***Samtidige forbindelser***	250	800
• ***Multiple SecurityAssosiation(SA)***	Ja	Ja
• ***Båndbredde håndtering***	Nei	Nei
• ***Leverandør spesifisert throughput***	10 Mbps/ som nettverkets	Samme som nettverkets
• ***Access kontroll som støtter***	RADIUS	RADIUS
• ***Bruker authentisering***	SecurID	SecurID, Cryptocard
• ***Data integritet/autentisering***	X.509 digitale sertifikater HMAC MD5/SHA-1	X.509 digitale sertifikater HMAC MD5/SHA-1
• ***Kryptering***	40/56 bit DES 168 bit triple-DES	40/56 bit DES 168 bit triple-DES
• ***Hardware kryptering***	CryptoCore ved ASIC/FPGA chips	ASIC
• ***Nøkkel-utveksling***	Diffie-Hellman	Diffie-Hellman
• ***Nøkkelhåndtering***	IKE ISAKMP/manuell	IKE ISAKMP
• ***Datakompresjon***	Ingen	Ingen
• ***Protokoller i tunnel***	IPSec AH/ESP	IPSec AH/ESP og SST
• ***Adresse skjuling***	Ja, ved bruk av ESP, men ikke i EIP modus	Ja både ved ESP og SST
• ***Vedlikehold prog. Interface***	WindowsNT/95	WindowsNT/95
• ***Vedlikeholds interface***	Front panel/ 10Base-T/RS232	RS232
• ***Vedlikholdsverktøy***	RavlinNodeManager	Shivas VPN Manager™
• ***Klient programvare***	RavlinSoftClient Emulerer Ravlin10 Unit	Shivas VPN Client™
Logging/Monitorering	Ja/SNMP(MIB)	Ja /SNMP(MIB)

12. Foretatte tester på VPN løsninger

Det er foretatt flere tester på VPN løsninger, og flere av disse finnes på Internett, som eksempel se ”IPSec-Compliant VPN Solutions” [44]. Etter gjennomgåelse av disse ser en at

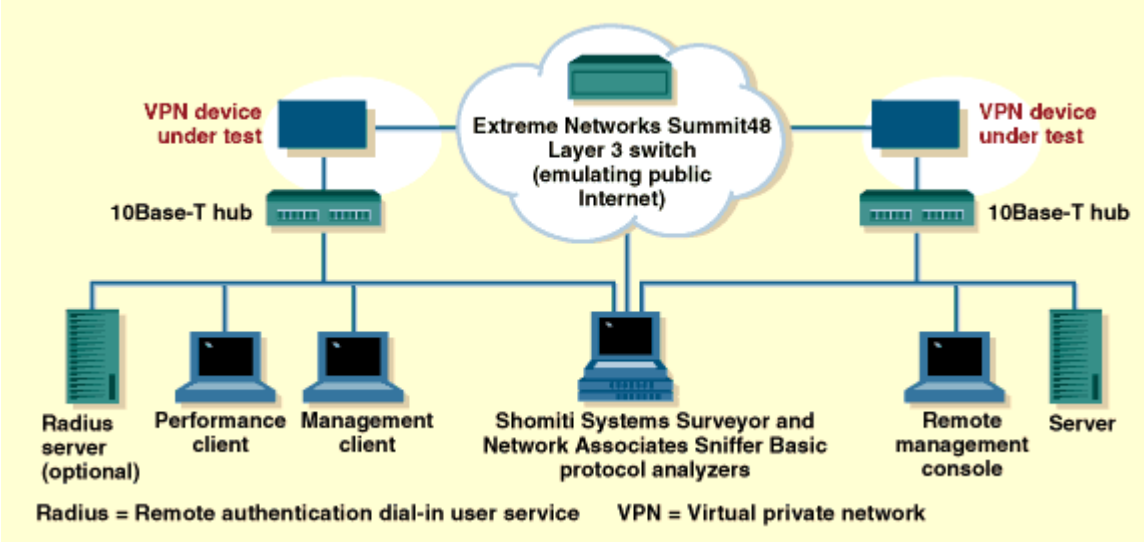
testene stort sett er utført med hensyn på ytelse. Magasinet Data Communications testgruppe [45] har utført en test hvor både Redcreeks Ravlin10 og Shivas LanRover VPN gateway er med. Her ble det testet sikkerhet, ytelse og hvor enkelt systemet er å administrere.

12.1 Testen

VPN løsningene i testen ble satt opp LAN-to-LAN, som vist på Figur 31.

Leverandørene som var med i testen måtte levere to utstyrsenheter med minst to 10Base-T interface og som supportet IPSec ESP, triple DES kryptering[46], meldingsautentifikasjon ved bruk av SHA-1 eller MD5, logging og fjern-administrasjons muligheter.

Testene ble kjørt i et miljø hvor to private subnett ble knyttet i lag over et emulert offentlig Internett.



Figur 31: Testkonfigurasjon

12.2 Sikkerhetstest

For å teste sikkerheten ble en Safesuite 5.0 fra Internet Security Systems Inc.[47] brukt.

Det ble kjørt flere enn 200 vanlige og ikke-vanlige angrepsforsøk mot hver enhet, fra f.eks. å oppnå super-bruker tilgang til å kjøre på med trafikk slik at enheten ikke kan håndterer lovlige forespørsler, såkalt denial-of-service angrep.

Men Safesuite fant ikke svakheter ved Ravlin10, mens LanRover VPN Gateway hadde en svakhet. Den tillot angripere å gjette TCP sekvens-nummerene, en svakthet som kan utnyttes for å skape trafikk som oppfattes å komme fra en ”trusted” maskin. På test-tidspunktet i juli 1998 var ikke Shivas klar over denne svakheten, men ville utarbeide en patch (en rettelse) så snart som mulig. Har dessverre ikke klart å finne ut om denne rettelsen i dag er tilstede. Til tross for at man på denne måten ikke kunne angripe VPN enhetene, kan de likevel ikke betraktes som helt sikre.

Testen ble utført utfra hittil kjente angrepsmetoder. I den virkelige verden, vil konfigurasjons feil og nye angrepsmetoder være tilstede. Derfor bør brukere betrakte sikkerheten som en prosess som pågår hele tiden, og utfra betydingen av denne for organisasjon, kjøre tester ved bruk av trafikkscanning og pågående avdekkings systemer.

12.3 Administrasjon verktøys funksjoner

Testen ble her utført ved å sammenligne konfigurerings og monitorerings mulighetene, og ble utført med fokus på to funksjoner; nøkkelhåndtering og administrasjon av enhetene, spesielt med hensyn på fjern konfigurering.

Flere oppgaver ble definert og hvor enkelt disse oppgavene kunne håndteres ble gitt karakterer fra 1 til 5, hvor 5 betyr enklest og 1 minst enkel.

Man tenkte seg et scenario hvor en nettverksasvarlig erfarer at en krypteringsnøkkel er blitt avslørt. Det foretrekkes at nettverksanvarlige ikke fysisk må være på sin arbeidsplass.

Administrator skulle ”fjernt fra” sørge for:
- at nøkkelen som er avslørt øyeblikkelig blir opphevet/tilbakekalt
- kontrollere at alle aktive sessjoner avsluttes eller avslutte de som ikke blir det
- stenge VPN enhetenes interface mot eksterne nettverk

Begge ”våre” VPN løsninger tillater at nøkler blir tilbakekalt/opphevet ”remotely” og nye nøkler kan fjern-generes. Det ble også konstantert at dette medførte at aktive sesjoner ble droppet og måtte reautentiseres. Interfaces kunne også stenges med fjern-kommando og derved nekte tilgang til nettverket.

At nettverksansvarlig kan sende kommandoer mot enhetene kommer av at VPN enhetene bruker kryptering ved konfigurasjons-sessjoner. Shivas bruker da en 112/168 bit implementasjon av Triple DES, mens RedCreek stoler på HMAC krypterings algoritmer.

Shivas skiller seg ut ved enkel håndtering under skifte av parametre/tilgangs-regler. Shivas enheten tilbyr også en planleggings mulighet, som tillater at nye regler trer i kraft en gang i fremtiden. Dette kan være hendig å bruke i perioder hvor nettverksansvarlige ikke er tilgjengelig.

Tabellen under viser hvordan RedCreek og Shiva kom ut i testen for administrasjon:

Sammenligning av VPN Administrasjon

Leverandør:	*Redcreek*	*Shivas*
Nøkkelhåndtering		
Mulighet for annulering/tilbakekallese fra fjern enhet (remote) ?	Ja	Ja
Letthet ved tilbakekalling av nøkkel	5	5
Tilbakekalling medfører at aktive sessjoner droppes ?	Ja	Ja
Hvor lett var det å droppe aktive sesjoner ?	4	4
Hvor lett ble nettverks tilgangen nektet ?	4	5
Enhets håndtering/administrasjon		
Sendes fjernkommandoer kryptert ?	Ja	Ja
Letthet ved eksekvering av fjernkommandoer ?	4	5
Droppes aktive sessjoner ved tillegging av nye regler (parametre) ?	Ja	Ja
Hvor enkelt er det å legge til nye regler ?	4	5
Reboot etter forandring ?	Nei	Nei
Generelt enkel håndtering ?	4	5
Karakterer: 1 = dårlig, 2 = OK, men ikke mer. 3 = god; 4= veldig god; 5 = ekselent		

12.4 Ytelse

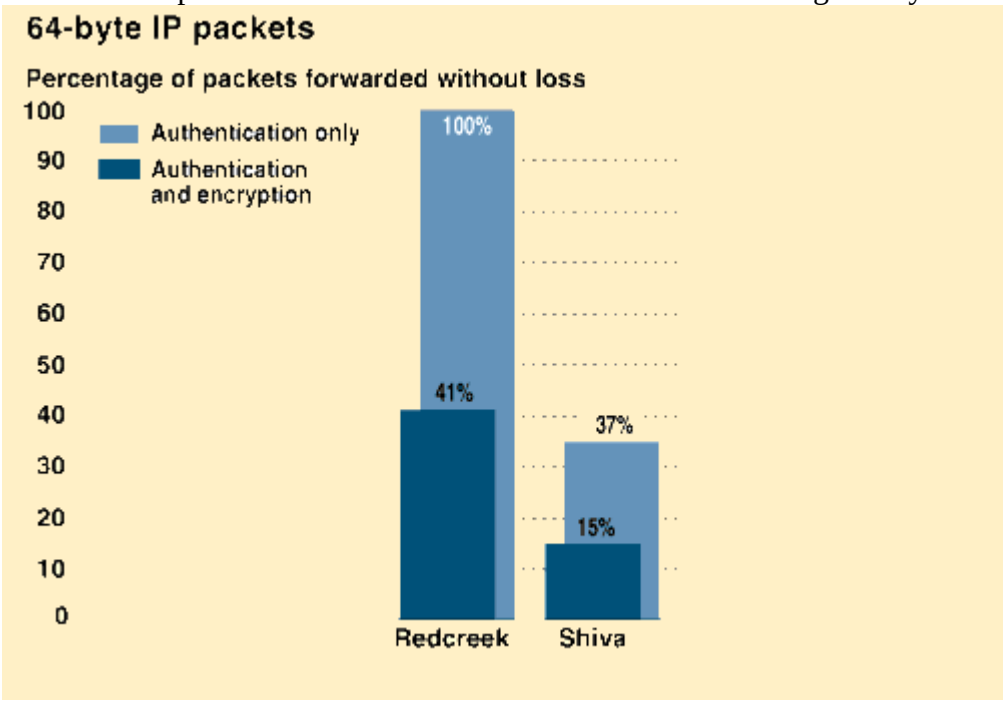
For å evaluere ytelse ble det kjørt trafikk mellom en maskin på det ene subnettet til en maskin på det andre subnettet. Maskinene på hvert private subnett rutet ikke, men de håndterte autentifikasjon og krypterings funksjoner, i tillegg til at det ble brukt RADIUS server for bruker autentisering.

Trafikken kjørtes i tunnel med IPSec ESP, kryptert med Triple DES på hver pakke, og autentifikasjon av pakkene ble gjort enten ved bruk av SHA-1 eller MD5 algoritmer. Det ble ikke brukt kompressjon eller omsetting av adresser. Bare Shivas støtter kompressjon.

"Throughput" ble målt for fire forskjellige pakkestørrelser, og til dette ble det brukt en Shomiti Surveyor [48] og Explorer [49] og en hardware-basert protokoll-analysator fra Shomiti System Inc.[50].

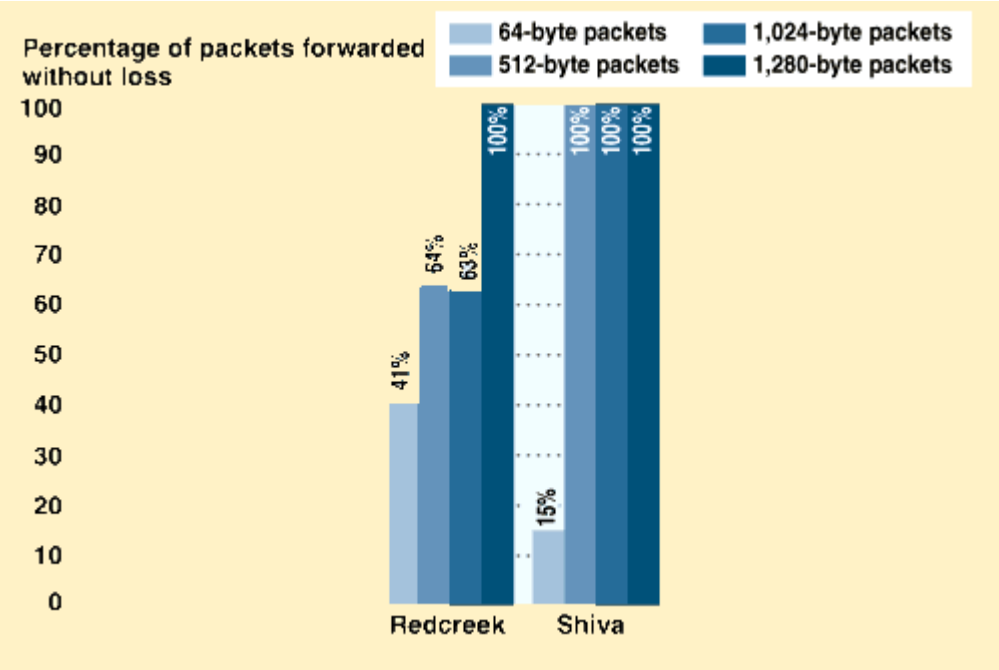
For å monitorere trafikken ble det bruken en Sniffer Basic fra Network Associates Inc. [51].
I testkonfigurasjonen ble det kjørt en pakkestrøm fra det ene subnettet til det andre over det offentlige Internett. Det ble brukt enveis trafikk for å få trafikken opp i netthastigheten uten kollisjoner mellom to VPN enheter. Trafikk-hastigheten ble målt ved hjelp av protokoll-analysatoren, både på sende og mottakersiden, og trafikken ble sendt bare med autentifikasjon og med både autentifikasjon og kryptering.
Resultatet av disse testene kan leses i Figur 32 og Figur 33.

Når Ravlin10 sendte videre flere enn 6000 pakker pr. sekund, stoppet sendingen med noen sekunders mellomrom (i ca. 4 sekunder), for deretter starte sendingen igjen. Denne "stopp og start" oppførselen er bannlyst for hastighets-sensitive applikasjoner som telefoni og video. Redcreeek tilskriver denne oppførselen til en "watch-dog" prosess som monitorerer enheten for sikkerhetsproblemer. Til tross for dette var Ravlin10's hastighet høyere enn Shivas.



Figur 32: Pakke-tap ved sending av 64-byte pakker.

Ytelsen var imidlertid bedre jo større pakker som ble sendt, også ved bruk av Triple DES kryptering, og oppnådde da hastighet opp mot nettverkshastigheten.



Figur 33: Prosent av sendte pakker uten tap ved sending av forskjellige pakkestørrelser

Det ble også gjort forsøk på å sende 1512 bytes pakker, som er det største pakkestørrelsen som tillates på Ethernet. Men VPN-enhetene sendte ikke pakkene videre uberørt, siden ESP headeren legger til overhead som gjør pakkene ulovlig lang. For å håndtere dette fragmenterte IP stacken pakkene i to, sendte fragmentene og reassemlet dem i mottakerenden. Alle fragmentene ble sendt i nettverkshastigheten.

12.5 Andre tester

Som i overnevnte test, framhever også andre at både Ravlin10 og LanRover VPN Gateway scorer høyt på yteleses måling. Tilsvarende er man fornøyd med administrasjonsmulighetene for begge produktene.

Blant annet har også PC Magazine utført en test på flere VPN produkter i november 1998 [52].

RedCreeks Ravlin10 får i denne testen bemerkning på at den ikke har egen støtte for CA (sertifiserings autoritet), at den ikke også fungerer som en brannmur og at det savnes større muligheter til å håndtere individuelle bruker tilganger. For å forbedre dette er den eneste muligheten å knytte til en RADIUS server. For å monitorere Ravlin10 enheten brukes som nevnt Ravlin Node Manager, som ble ansett som vanskelig i bruk.

Logging og statistisk informasjon blir positivt omtalt som lettlest og fullstendig spesielt med hensyn på detaljer i hendelses-meldinger og en nyttig MIB II[i] del for monitorering av SNMP trafikk. Konklusjonen, til tross for produktets nåværende mangler, er at med dens ytelse er RedCreek på riktig vei.

[i] MIB: Management Information Base, for bruk av nettverks vedlikeholds protokoller (SNMP) i et IP-basert nett. Se for mer informasjon: http://www.hitos.no/~ee/fag/datanett/snmp.pdf

Shivas LanRover VPN Gateway omtales negativt på grunn av høy pris. Det bemerkes at VPN Gatewayen bruker et propietært operativsystem som etter deres mening øker både sikkerheten og påliteligheten til produktet. I positivt retning teller også at produktet har inkludert brannmur, i tillegg kan en kjøpe et ”Hardware Accelator”-kort for å øke hastigheten og at produktet støttes med egen Certificate Authority (CA). Imidlertid viste det seg at i versjon 6,5 som ble testet, fungerte ikke denne CA i lag med IPSec. Nyere versjoner skal imidlertid gjøre det.

Oppsett av en VPN Gateway sies å være komplisert, og en remote klient konfigurasjon krevde mange parametre for å definere en tunnel. En slik konfigurasjon kan lagres og installeres over nettverket på hver maskin.

Brukertilgang-håndteringen er enkel, og det bemerkes som positivt at de fleste forandringer som gjøres på serveren lastes automatisk ned til klientene. Administrasjonsverktøyet er vindus-basert og benevnes som enkelt å lære og å bruke.

Positivt er det også at ved bruk av flere Shiva VPN Gatewayer kan disse konfigureres til å ta over for hverandre automatisk hvis feil oppstår i en av enhetene. Hvis en klient finner en tunnel med feil, vil denne gå i en liste over alternative tunneler som er konfigurert for denne klienten, for å finne et alternativ for å nå målet. Denne forandringen er transparent for brukeren.

Shiva VPN Gateway er best med et lite antall brukere (30 –40) og ved bruk av Triple DES. PC Magasine konkluderer med at ShivaVPN Gateway er en robust løsning som passer best i mindre organisasjoner.

12.6 Konklusjon: Ravlin10 og LAN Rover VPN Gateway

12.6.1 Redcreek

Ravlin10 er et godt valg for en liten organisasjon hvor de ikke innehar så mye teknisk ekspertise. Den er rimelig og lett å sette opp.

Ravlin10 kan konfigureres fra en frontpanel meny eller et meget enkelt administrasjon program, og grunnleggende VPN kommandoer som resetting av nøkler og blokkering av trafikken, kan utføres ved å trykke på en knapp.

Ravlin10 har god ytelese, og videresendte all trafikk i klartekst uten tap. Selv om Ravlin enhetene ville en gang imellom ta pause i 4 – 5 sekunder mens trafikken håndteres på grunn av en ”watch-dog” prosess, medførte det ikke store reduksjoner i ytelsen.

Ravlin forhandles i Norge av Merkantildata, og derfra har jeg fått de prisene som de foreløpig har. De minste Ravelin boksene (Ravlin 4) koster ca 15 000 kr. Ravlin 10 koster rundt 35 000 kr. Ravlin 100 kommer snart, og prisen på den er ikke helt avklart enda.

12.6.2 Shiva

Administrasjonsverktøyet for LAN Rover VPN Gateway er meget effektivt, og konfigurasjon og testing ble utført på mindre enn to timer. Det inkluderte et vidt sett av sikkerhetsfunksjoner, med planleggingsfasiliteten, for å sette inn valgte sikkerhetsfunksjoner på et senerer tidspunkt.

Det kan også utføre last-balansering hvis flere VPN Gatewayer er paralellt i bruk. Da vil trafikken automatisk fordeles over VPN gatewayene, som medfører jevn belastning over de enhetene som er i bruk.

Shivas selger også et separat Certificate Authority som jobber med produktet. Men LAN Rover har forutsigbare TCP sekvensnummer, som medfører at en angriper kan legge inn pakker som vil opptre som de kommer fra en sikker kilde. Shivas har imidlertid varslet at dette skal rettes på. Tilslutt, Shivas VPN løsning er dyr, og nesten dobbelt av andre tilsvarende produkter.

Har ikke funnet noen forhandler for Shivas i Norge.

Siden sikkeheten ofte er viktigere enn ytelsen i VPN sammenheng, og at de fleste applikasjoner produserer hovedsakelig store pakker, vil et VPN bygd opp rundt Ravlin10 eller LanRover VPN Gateway virke tilfredsstillende, til tross for at ”dagens” ytelse kan medføre redusert kvalitet for real-time applikasjoner.

13. Hvorfor og hvordan skal min bedrift velge VPN løsning ?

Siden en VPN-løsning må tilpasses den enkelte organisasjons særskilte behov finnes det ikke noe enkelt svar på hvorfor og hvilken løsning som skal velges.

Virksomheter som trenger en ”rimelig” skalerbar løsning for å møte etterspørselen for enkle og sikre kommunikasjonsmuligheter bør vurdere VPN. En slik løsning vil imøtekomme raske og uforutsigbare kommunikasjonsbehov mot medarbeidere som jobber mye ”ute”, avdelingskonterer og samarbeidspartnere. Samtidig må tilgangen til det interne nettverket skje uten at en er nødt til å gå på akkord med virksomhetens sikkerhetsbehov.

13.1 Fordeler med VPN

13.1.1 Kostnadreduksjon

Med VPN kan man oppnå besparelser på områder som kommuniksasjonskostnader, brukerstøtte, utstyr og vedlikehold, og samtidig oppnå større fleksibilitet, globalitet og at man bruker og betaler for ressuser ved behov.

- **Kommunikasjonskostnader (linjeleie og ”langdistanse” tellerskritt)**
  Å bruke Internett for å koble sammen to datamaskiner med stor avstand imellom, kan medføre vesentlige besparelser i forhold til dagens leide linjer og Frame Relay nettverk. VPN over Internett er også mindre kostbart enn en lang-distanse forbindelse. VPN er besparende, siden det muligjør at fjern brukere kan nå et ”langt-vekk” liggende nettverk ved bruk av tellerskritt til lokaltakst. Disse kostnadene antas å kunne reduseres med 50 %.

- **Utstyrskostnader**
  En annen fordel for VPN er at løsningen er meget fleksibel. En leid linje mellom to punkter gir bare tilgang til det lokale nettverket for den som fysisk er tilknyttet denne linjen. Et VPN medfører at ett tilknyttningspunkt kan betjene flere. Modem-pooler kan reduseres eller elimineres, til fordel for at all oppringt trafikk kan kjøres over en allerede eksisterende eller forsterket Internett-tilknyttning. Den samme Internett-tilknyttningen kan betjene både LAN-til-LAN kommunikasjon så vel som kommunikasjon med samarbeidspartnere, og ikke minst den vanlige Internett-tilgangen.
- **Brukerstøtte og teknisk støtte**
  I mange virksomheter hvor et mindretall av de ansatte er fjern-brukere, bruker disse en stor andel av systemansvarliges tid. IT avdelingene rundt om, støtter ofte fjern-brukere med et utall av forskjellige tekniske løsninger, og med utstyr som strekker seg fra analoge modemer til ISDN kort og kabel modemer. Ved innføring av VPN kan man oppnå en enhetlig løsning for alle fjernbrukere, og disse kan kobles opp via VPN'et mot det interne nettverket uten at de trenger kjennskap til dette. Driftskostnadene generelt kan reduseres i forhold til dagens løsning, og velger man en løsning med for eksempel en integrert brannmur, reduseres antall utstyr som må vedlikeholdes ytterligere.

13.1.2 Skalerbarhet

VPN medfører en umiddelbar mulighet for å tilpasse behovet med minimale anstrengelser. Virksomheter kan utvide kapasiteten, og nå deres medarbeidere, så enkelt som kjøpe eller bruke et eksisterende abonnement hos en Internett Service Provider (ISP). Siden det meste av oppsettet for klienten kan skje fra hovedkonteret, behøves heller ikke tekniske spesialister ute på de forskjellige lokasjoner. Dette innebærer at en ved behov, hurtig kan tilknytte seg nye brukere til de interne informasjonssystemene, og ikke som før vente i kanskje dager og uker for å få installert en leid linje eller Frame Relay. En må heller ikke glemme at et VPN kan nåes fra hele verden.

13.1.3 Støtte for "ad-hoc" samarbeidspartnere

I dag kan det for mange være av betydning å nå mange markeder og samarbeidspartnere raskt, og samtidig ha mulighet til å ofte å forandre mellom disse. Med VPN kan man nesten øyeblikkelig oppnå kommunikasjon med nye samarbeidspartnere og markeder, og forbindelser kan settes opp på ad-hoc basis med en hvilket som helst bedrift som har tilknyttning til Internett.

13.2 Hvordan velge

En organisasjon som vurderer å få en ny kommunikasjonsløsning mot eksterne brukere, det være seg å knytte seg mot en annen avdeling i virksomheten, fjern-arbeidere eller samarbeidspartnere, må analysere hvilke kommunikasjonsløsninger de har fra før, hvilke behov de har og hvilke krav som stilles til den nye løsningen.

13.2.1 Hva har vi fra før ?

Et ønske om noe nytt, bunner som oftest i at man ikke er fornøyd med dagens løsning. Når det gjelder kommunikasjon, må en først og fremst analysere det nettet en har bygd opp. En kan da stille seg spørsmål som:

- **Hvor mange fjern-brukere har vi ?**
  Hvis tilgangen utenifra til det lokale nettverket bare består av enkeltstående brukere, bør det klarlegges om dette antallet vil forandres fremover. Med modem-pooler vil en økning i antall fjern-brukere medføre ytterligere investeringer, og kanskje man dermed er bedre tjent med en ny enklere løsning for kommunikasjon med disse.
- **Mot hvilke lokasjoner har vi leide linjer/Frame Relay ?**
  Må vi ha tilgjengelighet til disse lokasjonene hele døgnet, med fast trafikkkapasitet, eller kan alle eller noen av disse forbindelsene erstattes av et VPN?
- **Hvor store datamengder skal transporteres eller hva bruker vi nettet til?**
  Her kommer det inn poeng som går på om en VPN løsning basert på Internett som det underliggende nettverk har mulighet til å gi den samme stabiliteten og tjenestekvaliteten som dagens løsning. Har vår virksomhet virkelig behov for en fast båndbredde eller brukes nettet stort sett til *ikke-forsinkelses-følsomme* applikasjoner ?
- **Hvordan er sikkerheten i dagens løsning ?**
  Et hvert nett kan avlyttes, og her må en vurdere om en er tjent med å kryptere trafikken på dagens nett, eller om en VPN løsning gir like god eller bedre sikkerhet
- **Har vi brannvegg ?**
  Kan denne eksisterende brannvegg fungere med den ønskede VPN løsningen. Hvis en ikke har brannvegg bør en vurdere en VPN løsning hvor brannvegg er inkludert.
- **Hvilken teknisk kompetanse har vi ?**
  Har vi nok intern teknisk kompetanse til å håndere og drifte et VPN, eller skal det velges en løsning som ikke krever for mye kompetanse (og hva medfører det), eller skal en outsource driften av VPN'et ?
- **Kostnaden med dagens løsning ?**
  Hvis kostnadene er det vesentlige punktet for å velge en ny kommunikasjonsløsning, må en ha fullstendig oversikt over kostnadene ved dagens løsning, for derved ha mulighet til å vurdere om et VPN virkelig utgjør noen kostnadsredusjoner.

13.2.2 Hvilke behov for sikkerhet har vi ?

Det har i den senere tid vært veldig fokusert på sikkerhet i forbindelse med datakommunikasjon. Enkelte mener til og med at IT-bransjen til tider er preget av et sikkerhetshysteri [i].

Sikkerheten i VPN er som før nevnt bygget opp rundt 4 konsepter
Autentisering: forsikre at data stammer fra kilden de hevder å stamme fra
Tilgangskontroll: forhindre ikke-autoriserte brukere tilgang til nettverket
Konfidensialitet: forhindre at ingen leser eller kopierer data når de transporteres over Internett
Dataintegritet: forsikre at ingen fikler med data når de transporteres over Internett

Med det overstående i tankene og momenter fra kapittel 5 er det naturlig å stille spørsmål rundt sikkerheten virksomheten.

[i] PC World Norge, Nettverk & Kommunikasjon nr. 3 1999

- **Er den informasjonen som vi utveksler interessant for andre ?**
  Hvor verdifull er den informasjon som din virksomhet utveksler over et offentlig nett for din virksomhet ? Er den verdifull for andre, og kan tilgangen til din virksomhets informasjon skade din bedrift ? Er denne informasjonen så verdifull at man kan forsvare investeringer for å sikre denne informasjonen ?
- **Er denne interne informasjon lett tilgjengelig internt i bedriften ?**
  Hvis sensitiv informasjon er lett tilgjengelig internt i bedriften, bør en vurdere sikkerheten internt først og fremst. Det hjelper lite å sikre informasjon som skal transporteres over et nett, hvis denne informasjon likevel er lett tilgjengelig på andre måter. Ta med at en slik sikring ikke bare er teknisk, men ligger like mye i opplæring og bevisstgjøring av de ansatte.
- **Pålitelighet**
  Siden VPN i dette dokument bygger på Internett som det underliggende nettverk, bør en være oppmerksom på at en på Internett opplever ting som pakketap, umotivert nedkopling og andre forstyrrelser. Dagens protokoller er bygget for å forhindre at pakker tapes og for å finne alternative veier ved brudd. Til tross for at forbedringer stadig utvikles må en likevel være klar over at slikt kan forekomme, men også ha med at dagens leide linjer og Frame Relay løsninger også kan bortfalle.
- **Tilgang til nettet**
  Er tilgangen til dagens nett for enkelt, og medført at uvedkommende har fått tilgang til nettet ? Hvilke ulemper vil slik uautorisert tilgang bety for bedriften ? Hvilket økonomisk tap vil det medføre hvis en inntrenger ødelegger deler eller all informsjon som er lagret, eller gjør inngrep slik at nettet ditt lammes ?
- **Forskjellige sikkerhetsbehov for forskjellige kommunikasjonsformål ?**
  En framtidig VPN løsning har mulighet til fleksibel tilgang, og muligheter for forskjellige sikkerhetsnivåer etter behov. Er dette en fordel i din virksomhet ?
- **Gir dagens løsning bedre sikkerhet ?**
  Hvis hovedkravet for datakommunikasjon er sikkerhet, må en selvsagt vurdere om en ny løsning gir større sikkehet, eller om den løsningen som en allerede har investert i kanskje er tjenelig sett i sammenheng.

13.2.3 Hver enkelt må velge

Å vurdere hvordan et VPN skal være for en bedrift eller hvilken leverandør man skal velge, kan ikke gjøres uten gode kjennskaper til bedriften, dens kommunikasjonsbehov og sikkerhetskrav. Konklusjon blir derfor, at hvis en er kommet fram til at VPN muligens kan være løsningen for din bedrift, må en i dag bruke tid på å sondere markedet.

Hvilke leverandører finnes, og hvilke løsninger har disse å tilby ?

Etter å nøye ha gjennomgått sin bedrift, og videre stilt krav til det ønskede VPN, blir jobben, alene eller i samarbeid med flere mulige leverandører, å finne den VPN løsningen som bedriften er tjent med. Her er det ikke bare snakk om tekniske løsninger, men også et spørsmål om investeringskostnader og senere kostnader til bruk og vedlikehold. En må også i den forbindelse ha med hvor enkelt og rimelig løsningen kan utvides. Videre bør en samle informasjon om leverandøren, og da ta hensyn til:

- leverandøren kompetanse på produktet og det fagfeltet som dette omfatter
- muligheter for service og support

- kan leverandøren eller andre kjøre kurs for den som skal drifte og vedlikeholde systemet i bedriften

En annen mulighet for å komme fram til en løsning, er å snakke med samarbeidspartnere eller tilsvarende bedrifter som har investert i VPN. Erfaringer de har hatt kan være en god veiviser, og en kan derved unngå fallgruber som andre har gått i.

Søk på Internett kan også gi tips og veiledning. Der kan man finne blant annet en 10 punkts plan på hvordan man "bygger" VPN. Denne 10-punktsplanen består av følgende momenter før valg:
1. kravstilling
2. man må tidlig ha ledelsen med på prosjektet
3. forsøke å finne de/det produktet som passer
4. teste ut de antatt beste produktene
5. anta størrelse på systemet

og etter at man har valgt:
6. finne ut lokalisering for VPN serveren
7. rekonfigurasjon av nettverkskomponenter som f.eks. brannmur
8. installere og konfigurere VPN'et
9. monitorere og vedlikeholde VPN'et
10. ta backup

Denne planen kan du lese på henviste link [53].

14. Case Study

På grunn av for liten kjennskap til en spesiell bedrift som kunne gi grunnlag for en "Case Study", har jeg heller valgt å referere fra en Case Study som er gjort av ***techguide.com*** som en del av et dokument "Virtual Private Networking: Maximizing Network Performance While Reducing Costs" [54]. Gjør oppmerksom på at case study'et ble sponset av Shiva.

14.1 JetForm Corporation

Dette "case study"et ble gjort hos JetForm Corporation [55]. JetForm Corporation hadde på det tidspunktet 15 kontorer spredt rundt hele verden, 550 ansatte og voksende etterspørsel fra 250 reisende medarbeidere. JetNet Internettworking Services, et selskap tilknyttet JetForm, fikk i oppgave å øke WAN og "remote access" ytelsesnivået for å imøtekomme behovet fra nåværende og nye sentraliserte forretningsapplikasjoner.

Målet for JetNet var klart: skaffe en enkel, skalerbar og sikker tilgang for alle ansatte fra uansett sted i verden. Målet og kravene førte til beslutningen om å gå bort fra den eksisterende Frame Relay og dedikerte kommunikasjonsløsningen.

14.2 Krav

Det ble utarbeidet et 10 siders krav-dokument som ble forelagt 6 sikkerhets leverandører. Det første kravet var å finne en VPN løsning som brukte standard-baserte krypteringsverktøy. Andre krav var:
- fjern-brukerne skulle kunne aksessere VPN'et fra en Windows95 eller WindowsNT 4.0 arbeidsstasjon
- sentralisert administrasjon av VPN'et

- brannmur muligheter
- CA under WindowsNT
- "Voice over IP"
- Intergrasjon av SecureID[56]

I tillegg skulle man finne en løsning som samlet hadde lave kostnader. JetForm ønsket videre en løsning som kunne gjøre bedriften i stand til å leve opp selskapets budskap som består i effektivisering av elektronisk kommunikasjon. To år tidligere var det installert en Frame Relay løsning, som ikke lengere var effektivt nok for bedriften utfra deres krav som også inkluderte:

- et "dial-in" VPN for de reisende medarbeiderne og hjemmebrukere
- et VPN fra hovedkontoret til avdelingskontorene
- brannmurssikkerhet for regel-basert tilgang til Internett

Et annet mål for Jetform med å innføre en VPN løsning var at man fra hovedkontoret skulle ha muligheten for å kontrollere uansett VPN enhet. I følge JetForm oppfyllte Shivas VPN Suite også dette kravet.

Det siste kravet fra JetForm var at VPN'et måtte kunne jobbe med ikke-registrerte IP-adresser. Systemansvarlige ønsket seg en løsning som var enkel å installere og ikke kom til å kreve at all JetForms programvare ble nødt til å skiftes ut eller forandres. Shivas VPN Suite opererer på det riktige laget i nettverks-stacken slik at applikasjoner ikke må modifiseres.

Det skulle også taes hensyn til at JetForm brukte Secure Remote Access (SRA) som involverer autentifiksjons ved hjelp av et kort, og at JetForm hadde planer om å åpne nettverket sitt for sine samarbeidspartnere gjennom et extranet.

14.3 Valg

JetNet fikk respons fra flere av de forespurte leverandørene, men valgte Shiva utfra at Shiva VPN Suite var den eneste løsningen som tilfredstilte de foreløpig kravene deres.

14.4 Installasjon og erfaringer

JetForm installerte Shiva VPN Client Software på noen bærbare PC'er og arbeidstasjoner på avdelingskontorer behov for fjern-aksess som piloter under implementasjonsfasen. I denne overgangs måtte JetNet forsikre seg om at ingen ville miste sine aksessrettigheter. Shivas støtte for SecureID gjorde at overgangen fra Secure Remote Access (SRA) (som involverer autentifiksjons ved hjelp av et kort) gikk uten problemer. Fjernbrukere kunne fremdeles bruke deres kort mens installasjon av Shiva VPN Client Software pågikk. JetForm bruker nå Shiva VPN Client Software med sertifikat for alle fjern forbindelser på det avdelingskontoret som var pilotkontor. Uttalelsene derfra var at salgspersonalet var fornøyd med den nye løsningen, og at den er pålitelig og oppfyller deres ønsker.

Målet for Jetform med å innføre en VPN løsning var også at en fra hovedkontoret skulle ha muligheten for å ha kontroll over uansett VPN enhet. I følge JetForm oppfyllte Shivas VPN Suite også dette kravet.

En av mange hindre for JetForm var båndbredde. Med hundrevis av ansatte som skal ha tilgang til Internett og deres intranett måtte tilgang til tilstrekkelig båndbredde være tilstede.

JetForms systemansvarlig konstanterte at Shivas løsningen ga tilgang til større båndbredde til en brøkdel av kostnadene som Frame Relay løsningen innebar. Han sier videre: ”Samlet har vi nå en bedre løsning som er lettere å drifte og med en ytelse som overgår den gamle.” Etter å ha sammenlignet reponstiden mellom det gamle frame relay nettet og det nye Shiva VPN Gateway, ble det fastslått at den nye løsningen hadde en høyere hastighet. Responstiden for frame relay nettverket var 340 - 350 ms, mens responstiden for Shiva VPN Gateway var 120 ms.

14.5 Kostnader

Systemansvarlig hos JetForm har analysert kostnadene. JetForm sparer $5,000 US/måned for hvert kontor i forhold til frame relay systemet. Kapitalkostnadene ved å kjøre et frame relay nettverk var for dem $243,000 per år. Med Shivas VPN Suite er kapitalkostnadene foreløpig antatt til å bli rundt $194,000.

Systemansvarlige hevder også at det har vært en merkbar nedgang i mengden av hardware som rekvireres rundt om til avdelingskontorene. Med sentrale databaser forsvant selvfølgelig nødvendigheten av å administrere databaser på hver av våre lokasjoner, og driften en remote-access-server ble borte. Alt som nå trengs er en lokal tilknyttning til en ISP og en sikker nettverkstilknytning mot hovedkontoret.

14.6 Konklusjon

Installsjon av Shivas VPN Suite pågår enda på noen av JetForms avdelinger. Frame relay løsningen er fjernet fra deler av nettverket og en full integrasjon var ventet å være ferdig i første del av 1999. Ved utgangen av 1998 ventet JetForm å utvide antall kontorer, og antok å få mere enn 500 fjern-brukere i nærmeste framtid. Så langt har Shivas VPN Suite fyllt deres krav og JetForm hadde på det tidpunktet som case-studien ble skrevet bare positive erfaringer.

15. Konklusjon

Virtual Private Networks skal erstatte dagens bedriftsinterne nett som er basert på oppringte samband og leide linjer.

Kravene til et slikt privat nett viser seg å kunne oppfylles.

En VPN løsning er i dag ikke spesielt rimelig, men likevel vil en VPN-løsning, på sikt, medføre kostnadsreduksjoner i form av mindre drift -og investeringskostnader. Et VPN krever mindre utstyr, mindre kommunikasjonskostnader i forhold til faste leide linjer og en enhetlig løsning for alle fjern-brukere i en organisasjon.

En VPN løsning er ikke ressurskrevende for driftspersonalet. Administrasjon og vedlikeholdet av et VPN, er enkelt med de medfølgende vedlikeholdsverktøy. Vedlikeholds- og administrasjonsprogramvaren som følger med de omtalte produktene i dette dokumentet, framstår for meg (med 10 års driftserfaring), som forståelig og lette å sette seg inn i.

Til tross for at det er forskjellige protokoller tilgjengelig til bruk ved bygging av et VPN, ser det ut for at IPSec blir standarden for fremtidige VPN. IPSec er blitt en sikker protokoll for kommunikasjon. Sikkerhetskravene som aksesskontroll, autentisering og hemmeligholdelse

blir oppfylt med IPSec, og et VPN kan betraktes som like sikkert eller sikrere enn et nett basert på leide linjer. Informasjonen kan selvfølgelig også krypteres på leide linjer, men ved at dette skjer i et VPN uten for mye aktivitet fra en klient, er en stor fordel.

I fremtidige IP nett med IPv6, hvor man får garantert tjenestekvalitet som bandbredde, vil VPN komme sterkere og kanskje bli den mest vanlige løsningen for bedriftsinternkommunikasjon over lange avstander.

Utviklingen pågår hele tiden innen dette området og VPN-produktene kommer stadig ut i forbedrede utgaver, både m.h.p. ytelse og håndtering. For en organisasjon med behov for en ny kommunikasjonsløsning med sine fjernbrukere, ville jeg valgt en VPN-løsning, forutsatt at man har vært igjennom de vurderinger som beskrives i dette dokument.

Referanser:

[1] Ferguson, P. and Huston, G. - "What is a VPN?", Revision, April 1 1998; http://www.employees.org:80/~ferguson/vpn.pdf

[2] "Making sense of Virtual Private Networks", Avential Corporation; http://www.avential.com

[3] "A Closer Look at Remote Access", Indus River™ http://www.indusriver.com/wpaper.pdf

[4] "A Framework for IP based Virtual Private Networks", <draft-gleeson-VPN-framework-00.txt>; http://ieft.org

[5] Check Point™ Software Technologies Ltd, March 23 1998; http://www.checkpoint.com/vpn/vpnwp.html

[6] "Angrep rettet mot svakheter i TCP/IP", Norman Data Defense Systems; http://www.norman.no/wp_smurf.htm

[7] "Quality of Service for Virtual Private Network", Cisco Systems Inc.; http://www.cisco.com/warp/public/cc/sol/mkt/ent/vpne/qsvpn_wp.htm

[8] "Quality of Service over IP: References", OSU Department of Computer and Information Science; http://www.cis.ohio-state.edu/~jain/refs/ipqs_ref.htm

[9] "IP Security Protocol (Ipsec)"; http://www.ieft.org/html.charters/IPSec-charter.html

[10] Socks resources; http://www.inet.no/dante/links.html

[11] I en løsning basert på SSL (spesifisert av Netscape), vil en melding som sendes mellom avsender og mottaker, kun tilfredstille krav til autentisitet og integritet på vei fra avsender og frem til mottakersystemet (mer presist mellom web-klient og web-tjener).

[12] "Point-to-point Tunneling Protocol", <draft-ieft-ppptp-07.txt>, http://ieft.org

[13] "Understanding PPTP", Microsoft Windows NT Server; http://microsoft.com/ntserver/commserv/techdetails/prodarch/understanding_pptp.asp

[14] "The Point-to-Point Protocol (PPP)"; http://www.ifi.uio.no/doc/rfc/rfc1661.txt

[15] "The PPP Encryption Control Protocol (ECP)"; http://www.ifi.uio.no/doc/rfc/rfc1968.txt

[16] "PPP DES Encryption Protocol"; http://www.ifi.uio.no/doc/rfc/rfc2419.txt

[17] "The PPP Compression Control Protocol (CCP)"; http://www.ifi.uio.no/doc/rfc/rfc1962.txt

[18] "Layer 2 Tunnel Protocol", Cisco System; http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.pdf

[19] "Layer Two Tunneling Protocol (L2TP)", http://info.internet.isi.edu/in-drafts/files/draft-ietf-pppext-l2tp-14.txt

[20] "Remote Authentication Dial-in User Service (RADIUS)" ; http://www.ifi.uio.no/doc/rfc/rfc2059.txt

[21] "Security Architecture for the Internet Protocol", nov. 1998; http://www.ifi.uio.no/doc/rfc/rfc2401.txt

[22] "IP Authentication Header (AH)", nov 1998; http://ietf.org/rfc/rfc2402.txt

[23] "Encapsulating Security Payload (ESP)", nov. 1998; http://ietf.org/rfc/rfc2406.txt

[24] " The MD5 Message-Digest Algorithm", http://ietf.org/rfc/rfc1321.txt

[25] "IP Authentication using Keyed MD5" ftp://ftp.isi.edu/in-notes/rfc1828.txt

[26] " Hashing Authentication Code (HMAC): Keyed-Hashing for Message Authentication; http://ietf.org/rfc/rfc2104.txt

[27] "The Use of HMAC-MD5 within ESP and AH", nov. 1998; http://ietf.org/rfc/rfc2403.txt

[28] ”Assigned Numbers RFC”; http://www.ifi.uio.no/doc/rfc/rfc1700.txt

[29] "Internet Assigned Numbers Authority (IANA)"; http://www.iana.org/

[30] "The ESP DES-CBC Transform"; ftp://ftp.isi.edu/in-notes/rfc1829.txt

[31] ”The Use of HMAC-SHA-1-96 within ESP and AH”; http://www.ifi.uio.no/doc/rfc/rfc2404.txt

[32] "IP Encapsulation within IP"; http://ietf.org/rfc/rfc2003.txt

[33] Hentet fra prosjektoppgave Virtual Private Networks av Gunnar Storebø, April 1998 http://www.idi.ntnu.no/~playboy/prosjekt/prosjekt.html

[34] ”Internet Security Association and Key Management Protocol (ISAKMP)” http://www.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-10.txt

[35] "The Internet Key Exchange (IKE)"; ftp://ftp.isi.edu/in-notes/rfc2409.txt

[36] RedCreek Communications; http://www.redcreek.com/pdf/Ravlin10.pdf

[37] Shiva Corporation; http://www.shiva.com/pdf/vpngateway.pdf og http://www.shiva.com/pdf/shivavpnconcepts.pdf

[38] ”Digital Signature Standard (DSS)”; http://jya.com/fips186.htm

[39] Diffie-Hellman Method For Key Agreement; http://www.apocalypse.org/pub/u/seven/diffie.html

[40] ”Internet X.509 Public Key Infrastructure”; http://www.es.net/pub/rfcs/rfc2528.txt

[41] Shivas Certificate Authority: http://www.lms.com.my/lms-td/config-vpn-ca.htm

[42] VLANs Usurped By Virtual Private Networks April 12, 1999; http://www.internetwk.com/

[43] **ICSA:** International Computer Security Association (tidligere NCSA). For å bli sertifisert av ICSA må produkter og systemer passere en omfattende sett av tester. ICSA gjennomfører fullstendige tester årlig og tilfeldige kontroller av produktenes seneste versjoner løpende. Kjøpere av ICSA godkjente produkter er sikret at de holder en viss kvalitet.

[44] ”IPSec-Compliant VPN Solutions”: Network Computing; http://www.networkcomputing.com/914/914r1.html

[45] ”VPNs: Safety First, But What About Speed?”: Magasinet Data Communication; http://saxophone.agora.com/lab_tests/first.html

[46] The ESP Triple DES Transform; http://www.ifi.uio.no/doc/rfc/rfc1851.txt

[47] ”Internet Security Systems”, http://www.iss.net/

[48] Shomiti Systems Inc. (San Jose, Calif.); http://www.shomiti.com/products/surveyor.html

[49] Shomiti Systems Inc. (San Jose, Calif.); http://www.shomiti.com/products/explorer.html

[50] Shomiti Systems Inc. (San Jose, Calif.); http://www.shomiti.com/products/products.html

[51] Network Associates Inc. (NAI, Santa Clara, Calif.);
http://www.nai.com/products/network_visibility/sniffer_basic/basic.asp

[52] ”Your Private Internett”, PC Magazine, november 1998;
http://www.zdnet.com/products/stories/reviews/0,4161,360486,00.html

[53] "Building VPN's: The 10-point paln", Tina Bird, Secure Network Systems;
http://www.data.com/tutorials/point.html

[54] "Virtual Private Networking: Maximizing Network Performance While Reducing Costs";
http://www.techguide.com

[55] JetForm Corporation; http://www.jetform.com/

[56] Secure Data Transfer (SDT) SecurID™; http://www.securitydynamics.com/fg_html/ns.html