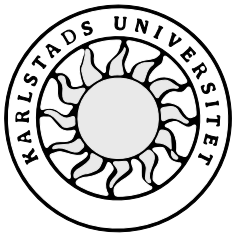


Datavetenskap

Charlotta Lagerkvist

Studie av VPN och dess tillämpning hos Karlstads kommun

Examensarbete, C-nivå

2000:20

Studie av VPN och dess tillämpning hos Karlstads kommun

Charlotta Lagerkvist

Denna rapport är skriven som en del av det arbete som krävs för att erhålla en kandidatexamen i datavetenskap. Allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och inget material är inkluderat som tidigare använts för erhållande av annan examen.

Charlotta Lagerkvist

Godkänd, 2000-06-08

Handledare: Hua Shu

Examinator: Stefan Lindskog

Sammanfattning

Denna rapport behandlar VPN (virtuella privata nät) och hur de passar in i en större organisation som exempelvis Karlstads kommun. Karlstads kommun hanterar varje dag sekretessbelagda uppgifter och behöver därför ett system som skyddar informationen från att hamna i fel händer. Idag skickas information helt öppet (okrypterat) över Internet, och då kan den som har rätt utrustning och kunskap få tillgång till allt som skickas. Internetanvändandet ökar och fler vill få möjlighet att arbeta på distans och nå arbetets intranät hemifrån på ett säkert sätt.

VPN används för att koppla samman arbetsplatser som är utspridda över stora geografiska områden. Det används även för att anställda hemifrån ska kunna komma åt hela intranätet som mail, interna sidor och filer där filstrukturen ser likadan ut på hemdatorn som på jobbet. VPN bildar en ”tunnel” mellan de som kommunicerar med varandra. I den tunneln krypteras all data, så att ingen utomstående kan läsa det som skickas. VPN delas in i tre grupper, mjukvarubaserade, hårdvarubaserade och brandväggsbaserade lösningar. De viktigaste aspekterna är kryptering, autentisering och undvikande av att utomstående kan ta del av nätverkets struktur.

Resultat från intervjuer och enkätundersökning i Karlstads kommun visar att behov finns av ett säkerhetssystem för säker åtkomst av intranätet hemifrån. Studie av befintliga VPN-lösningar visar att Karlstads kommun kan utnyttja VPN för att uppfylla sina krav. Exempel på en lösning som skulle passa för en organisation som Karlstads kommun beskrivs i rapporten.

Study of VPN and its employment at the municipality of Karlstad

Abstract

This paper is about VPN (virtual private networks) and how they fit into a big organization like for example the municipality of Karlstad. The municipality of Karlstad that every day handles secret documents needs a system to protect the information. Today information is sent without encryption over the Internet, which means that a person having the right equipment and knowledge can see everything that is sent. Now that the use of Internet is increasing, more people want to have the ability to work from home and have access to the companie's filesystem in a secure way.

VPN is used to connect workspaces spread all over the world and to let the employees have access to the companie's files and mail from home where the filestructure looks the same as at work. VPN builds a "tunnel" between those that communicate with each other. In the tunnel all data is encrypted to make it hard for unauthorized persons to understand. VPNs are divided into three groups, softwarebased, hardwarebased and firewallbased. The most important aspects are encryption, authentication and avoiding of unauthorized persons to see the structure of the network.

Results from interviews and inquiry at the municipality of Karlstad show a need of secure access to the intranet from home. This report shows that the municipality of Karlstad can use VPN to achieve their goals. A solution that would fit into an organization like the municipality of Karlstad is described in the report.

Innehållsförteckning

Figurförteckning

1 Inledning

Den här rapporten behandlar riskerna med att skicka information över Internet och VPN (virtuella privata nät) som används för att minimera dessa risker. Rapporten inriktas på hur VPN skulle passa in i en större organisation som exempelvis Karlstads kommun. Varje dag hanterar de sekretessbelagda uppgifter och eftersom Internet är publikt, vilket innebär att ett Internetabonnemang kan skaffas av vem som helst och även kan tecknas helt anonymt, så behövs ett sätt att skydda informationen från att hamna i fel händer.

Förr i tiden var inte informationssäkerheten ett lika stort problem som det är idag. Då räckte det med att låsa in hemliga dokument i ett kassaskåp. När kopieringsapparaten började användas blev det genast svårare att hålla reda på hur många exemplar det fanns av varje dokument. När utvecklingen sedan gick ännu längre och Internet kom, blev informationssäkerheten ett problem. Idag är det svårare att se till att obehöriga inte får tillgång till hemlig information som t.ex. skickas via mail över Internet.

Idag skickas den mesta informationen helt öppet (okrypterat) över Internet, så därför kan den som har rätt utrustning och kunskap få tillgång till allt som skickas. Med detta i åtanke förstår man att det är viktigt att skydda sina skickade meddelanden från personer som vill komma åt och kanske sabotera informationen. VPN är en enkel och relativt billig lösning på detta och flera andra problem som behandlas i rapporten.

VPN används för att koppla samman kontor som är utspridda över stora geografiska områden, och för att anställda hemifrån ska kunna komma åt intranätet med mail, interna sidor och filer där filstrukturen ser likadan ut på hemdatorn som på jobbet. För att ingen utomstående ska komma åt informationen som skickas mellan hem och kontor måste den krypteras.

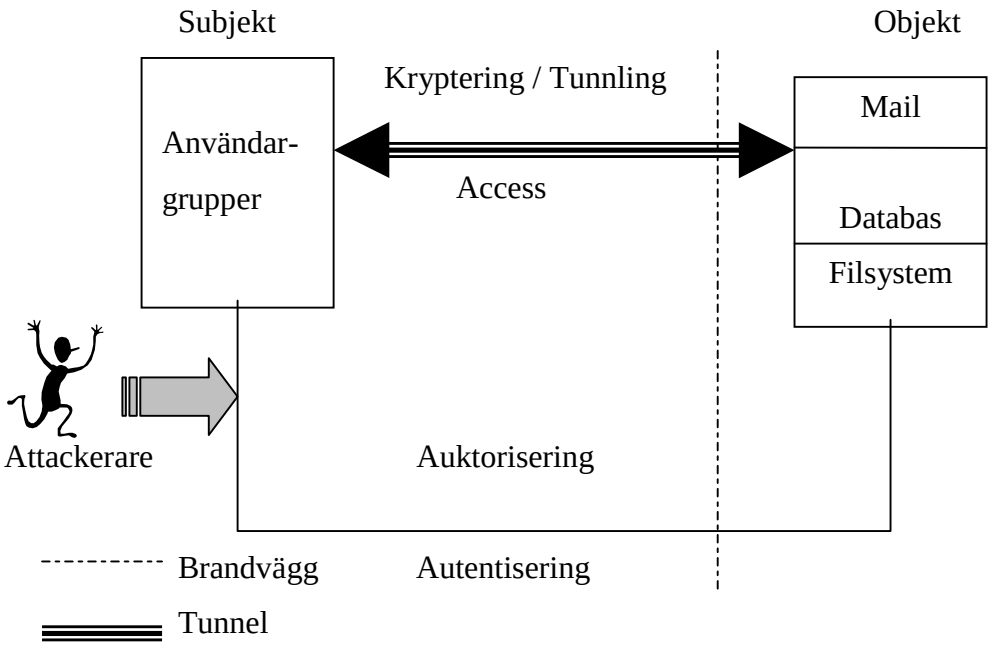
Den metod som används i studien är sökning av information via Internet, enkätundersökning samt intervjuer. I rapporten beskrivs först hur några VPN-lösningar fungerar och olika begrepp som VPN använder sig av, bl.a. tunnling och kryptering. Sedan kartläggs behovet hos Karlstads kommun idag och i framtiden. Det största önskemålet idag verkar vara att de anställda vill kunna komma åt arbetets filer, men framför allt sina mail hemifrån. Därefter undersöks hur VPN skulle passa in i organisationen. Rapporten avslutas med en slutsats där en VPN-lösning som är lämplig för Karlstads kommun beskrivs.

2 VPN och nätverkssäkerhet

2.1 VPN

VPN är ett sätt att kunna skicka data säkert över ett osäkert nät, t.ex. Internet. Det används av företag som vill att deras anställda ska få tillgång till intranät med mail, filer mm hemifrån. Det är även bra för företag vilkas anställda är utspridda över stora geografiska områden.

Namnet VPN kommer från att det är privat eftersom det är krypterat så att ingen utomstående kan läsa det som skickas, och virtuellt nät för att det för användaren ser ut som om han var ansluten till ett privat nätverk istället för ett publikt. Det känns alltså för användaren som om han satt på sin arbetsplats och var ansluten till det lokala nätverket där han kan komma åt mail och öppna filer på sitt konto.



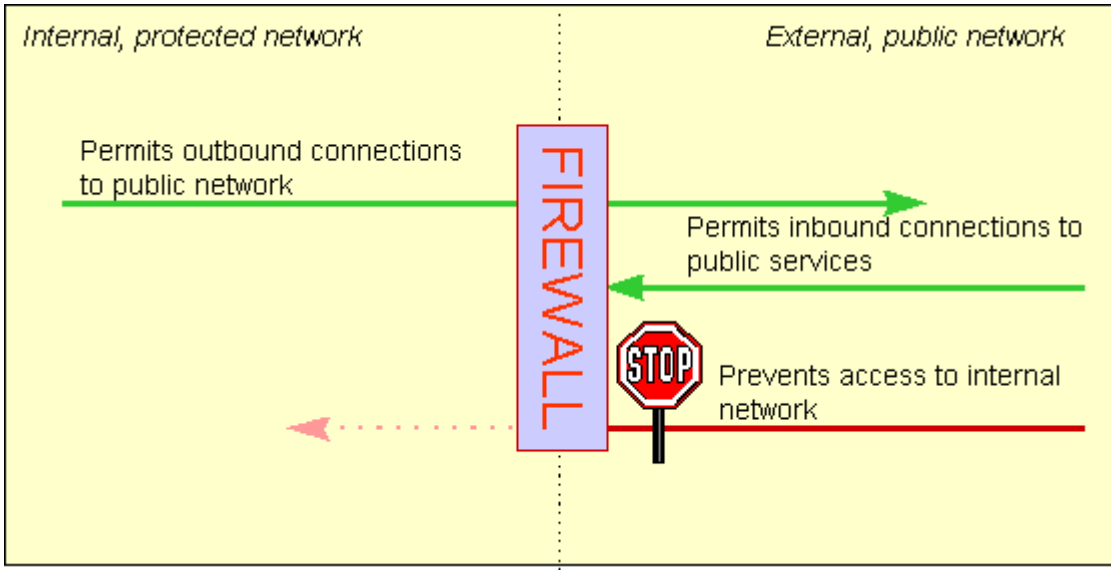
Figur 2.1 Illustrerar olika begrepp som VPN använder.

Figur 2.1 illustrerar vissa begrepp som VPN kan använda. Man kan dela in användarna, dvs subjektet, i olika grupper, beroende på vilka rättigheter de har mot objektet. Objektet kan t.ex. innehålla en mailserver, databas och filsystem. För att skydda objektet från attackerare (se 2.10) sätts ofta en brandvägg (se 2.2) mellan objektet och Internet. VPN fungerar genom att

det bildas en ”tunnel” mellan avsändaren och mottagaren (se 2.6). Tidigare kunde man få säkerhet genom att ha en fast koppling avsedd enbart för trafik mellan de ställen man ville koppla ihop, men det är oftast billigare att använda VPN. För att vara säker på att den man kommunicerar med verkligen är den som den utger sig för att vara krävs autentisering (se 2.7). Vill man kunna signera ett meddelande krävs auktorisering (se 2.8). För att skydda data så att ingen utomstående kan läsa det använder man kryptering som innebär att man byter ut meddelandet mot ett kodat (se 2.9). I följande avsnitt behandlas bl.a. begreppen i Figur 2.1 mer ingående.

2.2 Brandvägg (eng. firewall)

Namnet brandvägg kommer från de stenmurar man förr i tiden hade mellan husen för att förhindra att elden spreds från hus till hus vid en brand. På samma sätt kan man skydda sitt eget pålitliga nätverk från ett opålitligt, t.ex. Internet. Man kan också likna en brandvägg vid en ringmur som det bara finns en ingång genom och i porten står en vakt som kontrollerar om man får passera eller inte.



Figur 2.2 Brandvägg [16].

Idag använder många företag brandväggar för att skydda sitt nätverk. Brandväggen placeras mellan de båda näten. Som man kan se i Figur 2.2 ovan släpps ofta i stort sett all trafik inifrån det pålitliga nätet igenom, men alla inkommande paket kontrolleras. All trafik in mot det egna nätverket måste gå genom ett filter i brandväggen där det kontrolleras var paketen kommer från och vad de vill göra. Man jämför avsändaradressen med alla adresser i en accesslista över

godkända avsändare. Alla accessförsök till det pålitliga nätet från Internet hindras vanligtvis. En brandvägg skyddar bara förbindelser som går genom den, så det gäller att se till att det verkligen är enda vägen mellan näten. Den skyddar inte mot avsiktliga attacker inifrån intranätet. En brandvägg fungerar ofta så att från början är allt förbjudet, men man får ge rättigheter till vad som får göras genom att specificera exakt vilka paket som får passera. Ibland kan brandväggen bli en flaskhals i nätet eftersom den av säkerhetsskäl t.ex. kan förhindra att man kan hämta en fil med ftp.

2.3 Brandvägg vs VPN

Både brandväggar och VPN skyddar ett internt nät från t.ex. Internet. Men det finns stora skillnader mellan dem. En brandvägg spärrar obehöriga från att komma in i intranätet från Internet. VPN däremot ger vissa tillgång till intranätet via Internet, genom att skapa en tunnel där man skickar krypterad data.

Idag finns det brandväggar med inbyggda VPN-lösningar. I stort sett varje leverantör av switchar och brandväggar har en egen VPN-lösning.

2.4 IPSec

För att utrustning av olika slag och från olika leverantörer ska fungera tillsammans, måste man göra ett tillägg till IP. IPSec är en blivande standard med krypterad och autentiserad IP för säker privat kommunikation över Internet, [4]. Eftersom IPSec ännu inte är en standard så finns det flera varianter. Med hjälp av IPSec kan ett paket hitta rätt och komma fram oberoende av hur många noder det måste passera på vägen och vilken utrustning den passerar via interna nät, Internet, brandväggar och switchar.

De flesta VPN-lösningarna stödjer IPSec. Det är en samling protokoll som bl.a. stödjer användningen av kryptering, checksumma och elektroniska signaturer.

IPSec packar in datapaket i nya IPSec-paket. Två olika protokoll kan användas, AH (autentiseringsheadern) och ESP-header (encapsulation security payload), som ger stöd för autentisering och beskriver hur paketet är krypterat.

En version av IP-paket är IPv4-paket där headern innehåller information om avsändarens och mottagarens IP-adresser, som behövs för routing. Det kan lätt utnyttjas av en attackerare, eftersom IP-adresserna kan förfalskas genom sk ”IP-spoofing”. IPSec krypterar hela paket och håller därmed headerinformation och meddelande hemligt.

2.5 Möjliga VPN-lösningar

Det finns tre olika grupper av VPN-lösningar, hårdvarubaserade, brandväggsbaserade och mjukvarubaserade. Utbudet av VPN-lösningar ökar, och gränserna mellan de tre grupperna suddas ut alltmer då IPSec gör det lättare att kombinera olika lösningar. Att låta autentisering ske hos en Internetleverantör innebär att man måste ge leverantören information om hur verksamheten ser ut, och vilka som får göra vad. Det bästa är att bara ha sådan information på ett ställe, inne i den egna organisationen. Under denna punkt beskrivs de tre grupperna och sedan en lösning som har mjukvara på varje klient och en annan som har en autentiseringsdosa, där man slipper lägga in mjukvara hos dem.

2.5.1 Hårdvarubaserad VPN

De flesta hårdvarubaserade VPN-systemen är krypterande routrar. Fördelar med hårdvarubaserade lösningar är enkel användning och högst nätverks-throughput av alla VPN-system eftersom den inte slösar processoroverhead på att köra ett operativsystem eller andra applikationer. Därför bör lösningen väljas för överföringshastigheter över T1 (1.544 Mbit/s). Nackdelar med hårdvarubaserade VPN-lösningar är att de inte är lika flexibla som mjukvarubaserade system. De bästa lösningarna erbjuder mjukvaruklienter för fjärrinstallation och omfattar några accesskontrollformer som traditionellt hanteras av t.ex. brandväggar. Hårdvarubaserade lösningar tunnlar oftast alla trafiktyper.

2.5.2 Brandväggsbaserad VPN

Brandväggsbaserade VPN-lösningar utnyttjar brandväggens säkerhetsmekanismer såsom kontroll av vilka som har access till det interna nätverket. De utför även adressöversättning, stark autentisering, realtidsalarm och omfattande loggning.

Två av de mest använda konfigurationerna för VPN-lösningar är att köra VPN:

- parallellt med en befintlig brandvägg. Då krävs inte några förändringar av brandväggens infrastruktur, men man får två ingångar till intranätet. För att minimera säkerhetsriskerna släpper de flesta VPN-lösningarna bara igenom VPN-trafik och vissa har även förmågan att omdirigera övrig trafik till brandväggen.
- bakom en befintlig brandvägg. Här krävs förändringar av brandväggen. Den måste kunna konfigurera ett filter som låter VPN-trafik passera.

VPN kan även placeras framför eller i brandväggen.

2.5.3 Mjukvarubaserad VPN

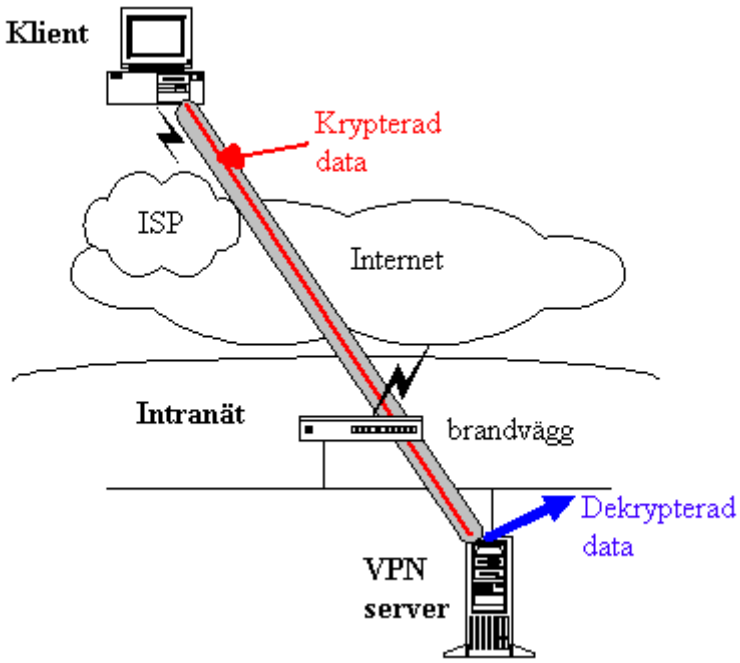
Mjukvarubaserade VPN-lösningar används om båda ändpunkterna inte kontrolleras av samma organisation eller om olika brandväggar och routrar är implementerade inom samma organisation. De är mest flexibla med avseende på hur nätverkstrafik hanteras. De flesta mjukvarulösningarna tunnlar trafiken baserat på adress eller protokoll. Denna lösning är alltså bra för organisationer som har olika typer av trafik, där inte alltid VPN och tunnling behöver användas. Att få access till organisationens intranät t.ex. kräver transport över VPN, medan vanlig surfning på Internet inte kräver VPN. Mjukvarubaserade lösningar är bästa alternativet om prestandakraven inte är höga, t.ex. användare som kopplar upp sig via modem. Mjukvarubaserade lösningar är ofta mer flexibla men svårare att hantera än krypterande routrar. Vissa kräver även att man gör förändringar i routingtabeller och nätverksadresser.

2.5.4 Exempel på VPN-lösning

Figur 2.3 illustrerar en VPN-lösning som är både brandväggsbaserad och mjukvarubaserad. Den fungerar på följande sätt:

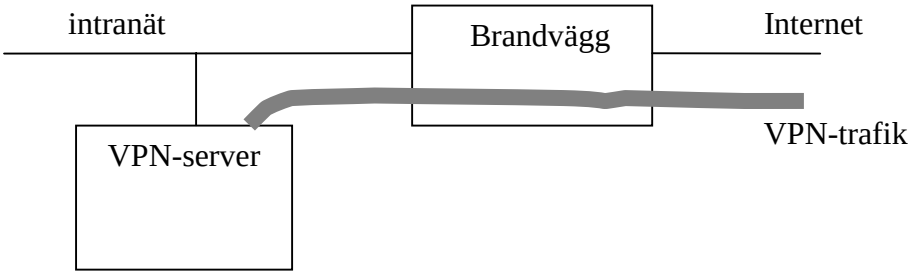
- Klienten som vill koppla upp sig ringer in till sin lokala Internetleverantör (ISP) och loggar in i ISP-nätverket.
- Vid uppkoppling mot intranätet initierar klienten en tunnelbegäran till VPN-servern som autentiserar användaren och bildar andra änden på tunneln [1].
- Innan klienten sänder data genom tunneln krypteras det med VPN-mjukvara.
- När VPN-servern får datat dekrypteras det och skickas vidare till mottagaren på intranätet. All information som skickas tillbaka till klienten krypteras innan det sänds över Internet.

[1] Med denna lösning har man en egen VPN-server, som bör placeras på IT-enheten, eftersom alla andra servrar finns där.



Figur 2.3 VPN-lösning med brandvägg och mjukvara.

Med denna lösning måste brandväggen kunna skilja på vilka meddelanden som ska gå till VPN-servern. För att inte belasta brandväggen för mycket kan en oanvänd port öppnas i brandväggen[2] (se Figur 2.4). Allt som kommer in genom den porten går direkt till en VPN-server som man måste ansluta. Servern kontrollerar vad det är som kommer, vem det kommer från och vad den vill göra och jämför det med rättigheterna man har. Är det OK, så skickas meddelandet vidare dekrypterat, annars kastas det.

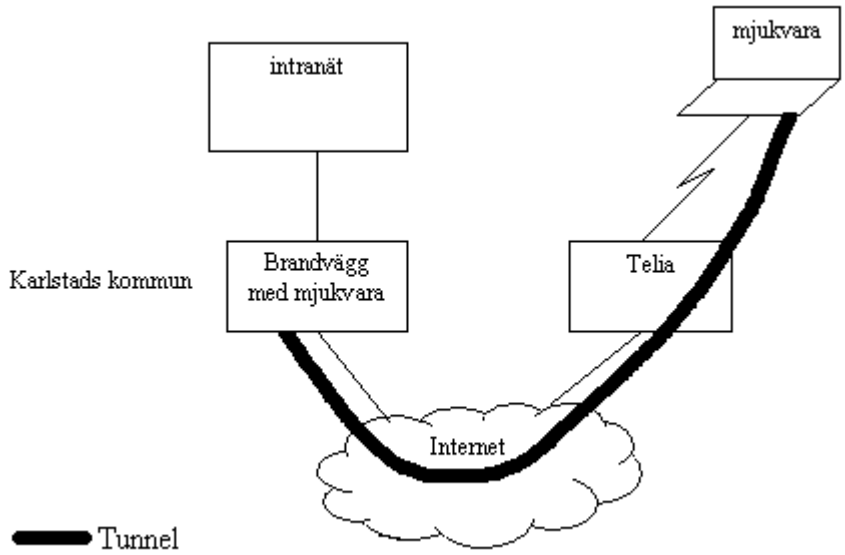


Figur 2.4 Unik port för VPN-trafik.

[2] Ett problem med det är att om man har satt samma port till t.ex. ftp, så kan någon utomstående komma in genom den porten, men om man ser till att inget annat använder den unika porten, så ska inget kunna inträffa.

2.5.5 Mjukvara på varje klient

VPN-mjukvara kan läggas in på alla klienter och även i Karlstads kommuns brandvägg[3]. Programvaran krypterar hos den som skickar och dekrypterar hos mottagaren.



Figur 2.5 VPN-lösning med mjukvara på varje klient.

Antag att en användare sitter med sin hemdator och kopplar upp sig med modem mot t.ex. Telia. När användaren vill koppla upp sig med Karlstads kommuns VPN bildas en ”tunnel” mellan användarens dator och brandväggen (se Figur 2.5). Det smidigaste sättet är att ge varje användare som ska ha tillgång till programvaran en diskett/cd-skiva för att installera hemma. Ett problem med att ha mjukvara på varje klient är var man ska lägga supporten för klienterna. Antingen kan IT-ansvarig på varje förvaltning ha ansvar för att mjukvaran är rätt konfigurerad och ligger på rätt ställe, eller så kan ansvaret ligga hos IT-enheten.

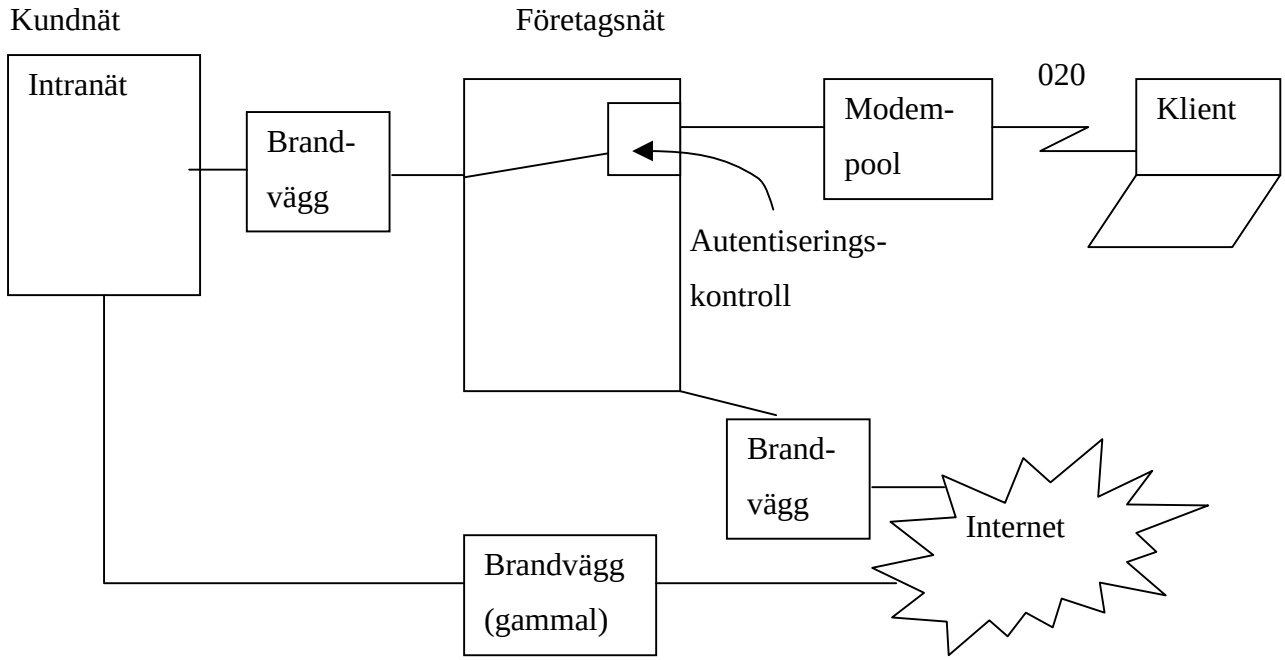
2.5.6 Smartcardlösning

Ett alternativ som Örebro kommun har skaffat och är nöjda med är en smartcardlösning. Här slipper man lägga in en mjukvara på varje datorklient. Istället får varje anställd en smartcarddosa (se punkt 2.7.2) med en personlig PIN-kod. Figur 2.6 illustrerar en smartcard-lösning där autentisering sker i ett företagsnät. Man loggar in genom att ringa upp en modempool med ett 020-nummer. Man ansluts sedan mot ett speciellt företagsnät istället för direkt mot Internet. Via det nätet kan man, efter autentisering med dosan, koppla upp sig mot

[3] Enligt WM-datas lösning.

det egna intranätet med VPN. För att komma ut på Internet kan man fortsätta att använda sin befintliga brandvägg eller välja att använda den brandvägg företagsnätet har mot Internet. Oftast blir det billigare att ha kvar sin gamla brandvägg, men det blir mer att underhålla.

Kostnaden för lösningen är anslutningen till företagsnätet som vanligtvis är en anslutningsavgift och en årsavgift, lokalsamtalskostnad och kostnad för varje dosa[4]. Någon bör vara ansvarig för att registrera vem som har vilken dosa för att kunna spärra om den förkommer.



Figur 2.6 VPN-lösning med smartcard.

Med denna typ av lösning måste man köpa in sig i ett företagsnät, men IT-enheten vill själv ha kontroll och kunskap över det som används. Ett syfte med VPN är att dölja nätverkets struktur för utomstående. För att slippa ha information om nätverket utanför den egna organisationen kan man låta autentisering ske i intranätet istället för i företagsnätet. Då slipper man även ha ett speciellt telefonnummer för att använda VPN. Detta alternativ kan vara dyrare än det som visas i Figur 2.6 eftersom det krävs att man skaffar en egen VPN-server. Föreningssparbankens lösning är ett exempel på en smartcardlösning.

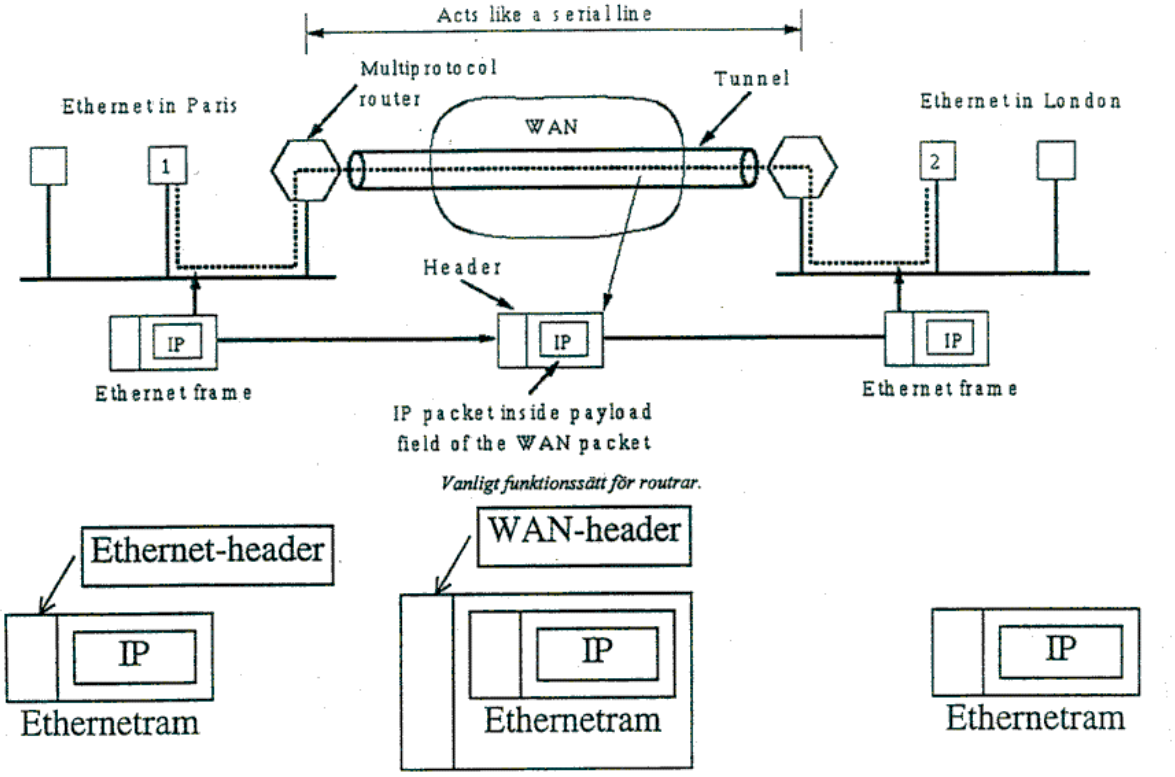
[4] Årsavgift skulle kunna ligga hos IT-enheten. ”Ticket” (lokalsamtalskostnad) och kostnad för varje dosa kan ligga på varje förvaltning. I priset för varje dosa kan ingå att leverantören har kontroll över vem som har vilken dosa, och kan spärra den om den förkommer, så att ingen annan kan använda den. Men det skulle IT-enheten kunna göra själva också.

2.5.7 Cockies

Vissa VPN-lösningar använder sig av att lagra cockies på användarnas datorer för att vara säkra på dess identitet. En cockie är en liten textfil, cockiefil, som placeras på hårddisken i användarens dator. Cockiefilen innehåller information om personen, vilka inställningar datorn har och vilka sidor man har besökt. Det är bara den webbplatsen som har skapat cockien som kan läsa den. Den används sedan för att kunna visa lämplig information nästa gång man besöker samma sida. Att acceptera en cockiefil innebär alltså inte att man ger den tillgång till sin dator, för den kan bara lagra information som man har skrivit till webbplatsen.

2.6 Tunnling på Internet

När man vill koppla samman två nätverk av samma typ, så kan det göras genom tunnling, även om det är en annan typ av nätverk mellan dem. Det går till på följande sätt. Man tar paketet som ska skickas och packar in det i ett nytt paket med en ny header som den andra typen av nätverk kan tolka. Sedan skickar man det över det främmande nätet, och när det kommer fram till andra sidan packas det upp och ser då ut precis som när man skickade det. Man kan se det som att man skickar meddelandet genom en ”tunnel” från router till router. Detta kan liknas vid att köra bil genom en tunnel där bara tåg får köra. Då får man köra fram bilen till början av tunneln. Där får man köra upp sin bil på tåget, som kör genom tunneln, och på andra sidan av tunneln kör bilen av tåget. Bilen har inte förändrats under tiden den stod på tåget. Det enda som hände var att den transporterades med hjälp av tåget. På samma sätt är det när man har tunnling. Man har ett ursprungsmeddelande (bilen) som man packar in i ett nytt paket (kör på tåget). Sedan transporteras det nya paketet genom tunneln och på andra sidan packas det ursprungliga meddelandet upp (kör av tåget). På detta sätt kan alltså ett paket gå genom vilka nätverk som helst.



Figur 2.7 Tunnling, [5].

VPN sätter upp en tunnel mellan två enheter som innehåller VPN-programvara. Däremellan krypteras meddelandet för att få största möjliga säkerhet. Det krypteras hos den som sänder och dekrypteras hos mottagaren. Det är bara trafik som går mellan VPN-programvarorna som krypteras, vilket innebär att trafik som ska till en annan destination kommer att sändas helt utan kryptering. Det är viktigt att ha i åtanke då man sänder information över Internet, att inte allt blir säkert bara för att man har skaffat VPN. Det som inte kommer att gå mellan VPN-anslutningar bör gå genom en brandvägg för att skydda nätet från obehöriga. För att vara säker på att det är rätt person man har kontakt med krävs autentisering.

2.7 Autentisering

För att kunna använda VPN måste man autentisera sig, vilket innebär att man bevisar för datorsystemet vem man egentligen är. Syftet är att man inte ska nekas några av sina rättigheter. Det finns ett flertal olika metoder och de vanligaste kommer att behandlas nedan. Vilken metod man väljer beror på hur verksamheten ser ut. Det kan vara lämpligt att använda olika autentiseringsmetoder på olika ställen i verksamheten.

2.7.1 Lösenord

Lösenord bör bytas ofta och inte ha anknytning till något som har med personen att göra. Man ska t.ex. inte använda sitt barns namn eller personnummer, som är lätt att gissa sig till. Istället bör man blanda bokstäver och siffror. Det finns speciella program som man kan testa sitt lösenord med för att se om det är lätt eller svårt att knäcka, och även program som kan gissa sig till lösenordet. Om lösenordet skickas okrypterat så kan någon använda ett så kallat snifferprogram där man kan ”sniffa” sig till vad lösenordet är. Därför är det bättre att skicka alla lösenord krypterade. För att öka säkerheten kan man t.ex. tillåta max tre felaktiga inmatningar av lösenordet.

2.7.2 Smart card

Smartcard är en miniräknarliknande dosa som kan användas vid inloggning och autentisering. Man går in på en webbsida där det vanligtvis står ett kontrollnummer som man får mata in i sin smartcarddosa efter att man slagit in en personlig PIN-kod i dosan. Av kontrollnumret genererar dosan ett lösenord som man får mata in på webbsidan för att kunna logga in. Vanligtvis är lösenordet endast giltigt en begränsad tid, t.ex. 3 minuter. Det kan även vara bra att ha automatisk utloggning om dosan varit inaktiv i t.ex. 1 minut. Detta för att minimera risken att någon utomstående kan få tag på dosan när den är påloggad. Denna autentiseringsmetod är bra ur säkerhetssynpunkt då det är mycket svårt att knäcka algoritmen. En negativ aspekt är att om det är många användare så kan det bli dyrt att använda denna metod eftersom varje dosa kostar ca 700 kr/st[5]. Ytterligare en negativ aspekt är att det kan vara svårt att hålla reda på dosan och komma ihåg lösenordet.

2.7.3 Kortläsare

Med kortläsare får alla användare ett eget passerkort som ger tillgång till fördefinierade salar och datorer med VPN. Vissa tider på dygnet kan det räcka att dra kortet genom kortläsaren, men andra tider måste man dessutom knappa in en personlig kod i kortläsaren. Det finns kort med magnetband eller mikrochips. Om man behöver lagra mycket information på kortet så är det bäst med mikrochips. Nackdelar med båda typerna av kort är att de kan slitas ut eller tappas bort och man måste ofta komma ihåg en kod. Kortläsare är olämpligt att använda hemma, då det är dyrt att installera.

[5] WM-datas alternativ.

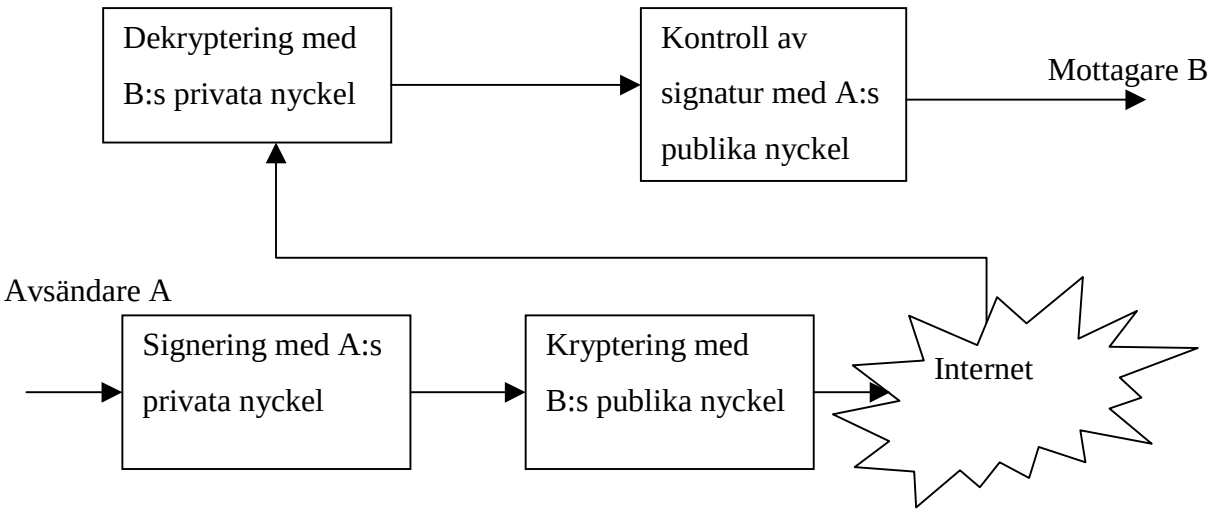
2.8 Auktorisering

Auktorisering innebär till skillnad från autentisering att man håller reda på vad varje användare får göra så de inte kan förneka sina skyldigheter. Det kan vara aktuellt om man vill bevisa att ett meddelande verkligen kommer från en viss avsändare. VPN kan använda sig av auktorisering.

2.8.1 Digitala signaturer/elektroniska underskrifter

Förr kunde avsändarens namnteckning bevisa dennes identitet med hjälp av handstilsexperter, men när man skickar digitala meddelanden krävs en ny typ av identifiering.

Digitala signaturer används för att juridiskt binda en avsändare till ett dokument, [1]. Det går till på följande sätt, se Figur 2.8. När en person skickar ett meddelande så skickas även en krypterad signatur med. Den består av en kontrollsumma som kan härledas från meddelandet och som är krypterad med hans privata nyckel. För att bevisa att han verkligen skickat meddelandet, går man in på den dator som meddelandet skickades till och kontrollerar signaturen som har sparats där. Sedan dekrypteras den med avsändarens publika nyckel. Är det samma meddelande kan han bindas till det. Då kan man konstatera både att han har skrivit det och att det inte har förändrats på vägen. Ett problem med detta är att om han ändrar sin nyckel, så går det inte att bevisa något, [5].



Figur 2.8 Signering i ett asymmetriskt system

För nycklar i digitala signaturer använder man 512 eller 1024-bitars nycklar.

Om ett meddelande ska arkiveras en längre tid, så kan man behöva göra om den digitala signaturen med jämna mellanrum med en giltig nyckel, eftersom det kan hända att någon knäcker krypteringsnyckeln, [6].

PKI (public key infrastructure) är en infrastruktur som stödjer användningen av elektroniska underskrifter.

2.9 Kryptering

Kryptering används för att förhindra att andra ska kunna stjäla eller ändra information som man skickat över Internet. Det innebär att man med hjälp av en speciell krypteringsnyckel ersätter den riktiga texten med en annan text som genereras med en algoritm. Beroende på hur viktigt det är att ha säkerhet kan olika starka krypteringsnycklar användas för att förhindra att någon annan kan läsa det som skickas. Man mäter längden på en krypteringsnyckel i bitar. En vanlig nyckellängd är 64 bitar men 128 bitars kryptering är att rekommendera idag. En nyckel på 64 bitar innebär 2^{64} olika möjligheter.

Även om mjukvarukryptering är 1000 ggr långsammare än hårdvarukryptering kan ändå en dator göra 250 000 krypteringar/sekund, [1].

Förr användes enkla algoritmer och för att kompensera det hade man långa nycklar. Idag är det tvärtom, dvs man använder kortare nycklar och svåra algoritmer, så även om en attackerare har tillgång till att få en valfri text krypterad, så ska det vara mycket svårt att komma på algoritmen.

Man skiljer på symmetrisk och asymmetrisk kryptering. Symmetrisk kryptering är 100 till 1000 ggr snabbare än asymmetrisk kryptering, [1].

2.9.1 Asymmetrisk kryptering

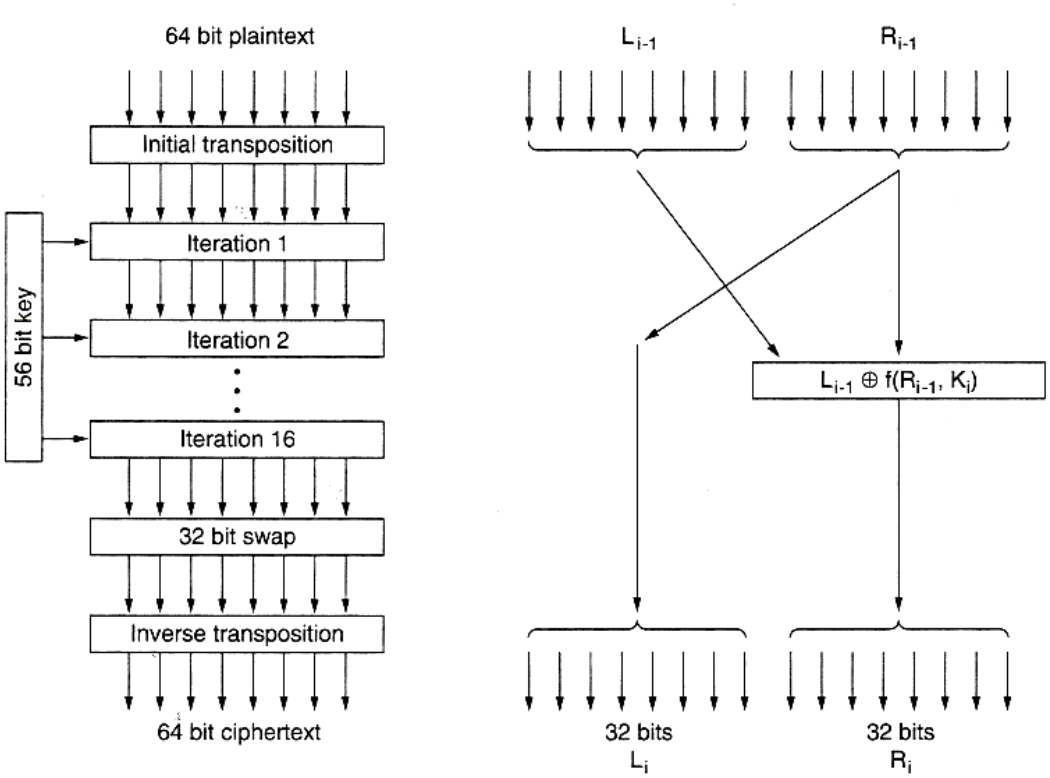
Grunden i asymmetrisk kryptering är att kryptering och dekryptering sker med olika nycklar. Det fungerar på följande sätt. Det som krypterats med den ena nyckeln kan bara dekrypteras med den andra nyckeln och vice versa. Det krävs alltså 4 olika nycklar för att två ska kunna kommunicera med varandra. Man får fram nycklarna med hjälp av en slumptalsgenerator som ger ett slumptal som i sin tur matas in i en matematisk formel som genererar nycklarna. Man väljer en nyckel som man kallar privat som man håller hemlig. Den andra, som kallas publik nyckel, kan man publicera och ge till vem som helst, för det är i stort sett omöjligt att komma på den privata nyckeln med hjälp av den publika. I asymmetrisk kryptering slipper man problemet med att distribuera hemliga nycklar. En metod som använder sig av asymmetrisk kryptering är RSA Digital Certificate (se punkt 2.9.3).

2.9.2 Symmetrisk kryptering

Symmetrisk kryptering är symmetrisk som framgår av namnet. Det vill säga man har samma nyckel för både kryptering och dekryptering. Detta är inte så bra ur säkerhetssynpunkt, då man inte i efterhand kan bevisa vem som var meddelandets avsändare respektive mottagare, eftersom båda använder samma krypteringsnyckel. Ett annat problem är att varje nytt par som ska kommunicera med varandra måste ha en ny krypteringsnyckel som måste distribueras säkert mellan dem.

2.9.2.1 DES

DES (data encryption standard) använder sig av symmetrisk kryptering. 1977 blev DES, som är en krypteringsalgoritm från IBM, standard för USA:s regering, [1]. Det användes ofta i industrin för säkerhetsprodukter. I en något modifierad form är det fortfarande användbart. I DES skickar man in 64 bitars klartext och genom olika iterationer får man ut en 64-bitars krypterad text. Vänstra delen av Figur 2.9 visar hur iterationerna går till. Den högra delen visar en iteration ingående.



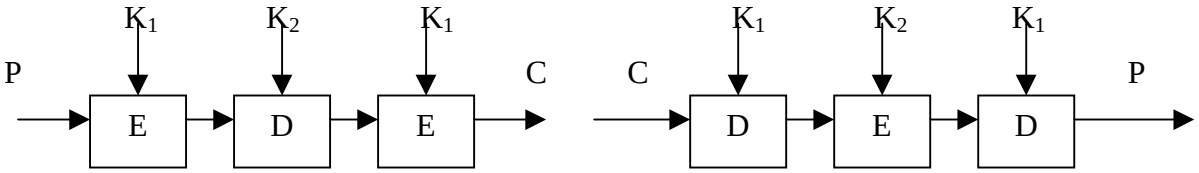
Figur 2.9 Iterationerna i DES, [1].

Det unika med DES på sin tid var att den inte bestod av bara en algoritm, utan av en hel familj av algoritmer, 2^{64} stycken. Egentligen har algoritmen 64 bitar, men det används inte mer än 56, för var åttonde bit är en s.k. paritetsbit. En paritetsbit används för att se så att inte data förändrats på vägen. Det finns udda/jämn paritet som kontrollerar antalet ettor/nollor. Problem med t.ex. jämn paritet är att felet endast upptäcks om det är ett udda antal fel. Är det två fel märks det inte, för då blir ändå paritetsbiten samma som om det inte varit något fel. För att använda algoritmen räcker det med att utbyta nyckeln. Det finns algoritmer som är betydligt snabbare än DES, t.ex. RC2, RC4 och RSA Data Security, [2]. DES har ansetts vara både långsam och sårbar, så därför vill man byta ut den mot t.ex. IDEA (se 2.9.2.3).

Merkle och Hellman (1981) har utvecklat en metod som kan knäcka dubbel kryptering, så det är inte mycket säkrare att köra DES två gånger efter varandra, [1].

2.9.2.2 Triple-DES

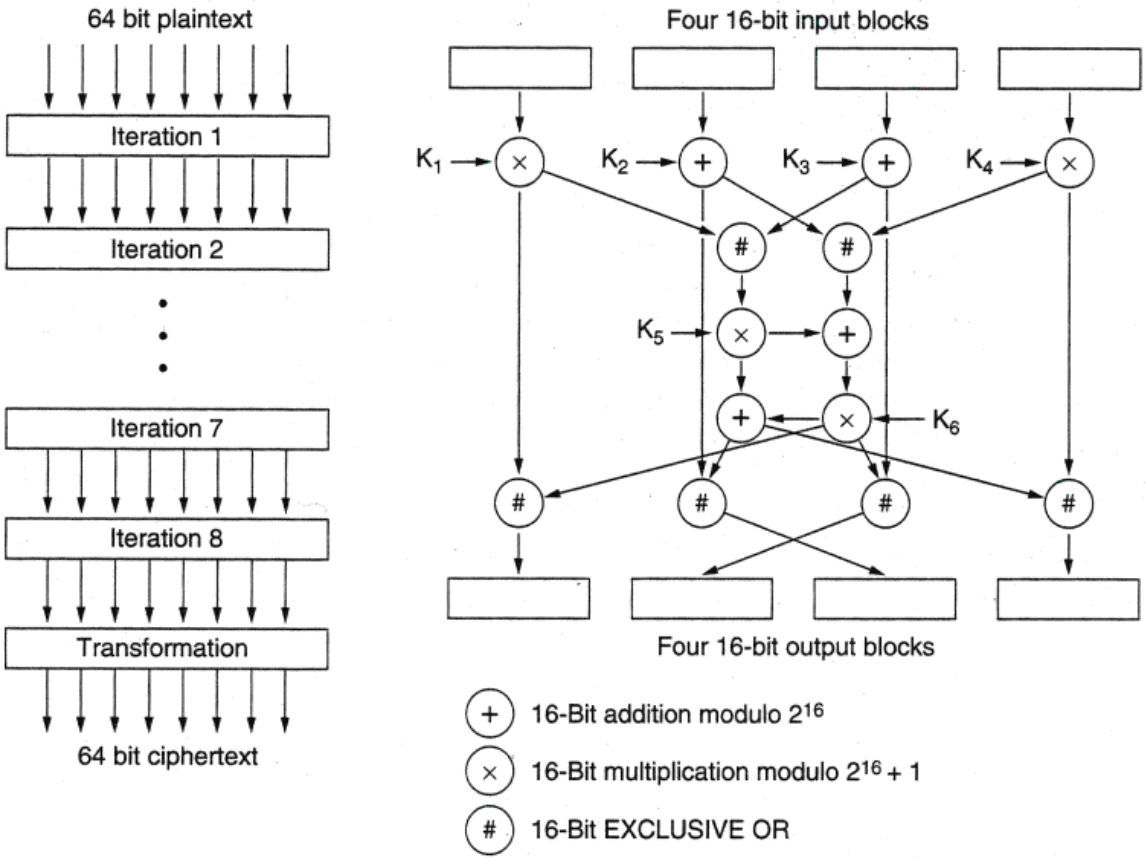
Triple-DES, eller 3DES som den också kallas, anses av många vara säkrare än vanlig DES. Skillnaden är att 3DES använder sig av DES tre gånger. Den krypterar meddelandet P med en nyckel K_1, dekrypterar med en annan nyckel K_2 och krypterar igen med nyckel K_1 och får fram det krypterade meddelandet C (se Figur 2.10). När man vill få tillbaka det ursprungliga meddelandet P från C gör man tvärtom. Man dekrypterar med K_1, krypterar med K_2 och dekrypterar med K_1, [1]. Om man sätter $K_1 = K_2$ kan datorn även kommunicera med en dator som använder sig av enkel DES-kryptering.



Figur 2.10 Triple DES

2.9.2.3 IDEA

IDEA (international data encryption algorithm) lanserades 1991, d.v.s. är betydligt nyare och även matematiskt bättre än DES, [2]. Den använder en 128-bitars nyckel. I IDEA skickar man in 64-bitars klartextblock och får ut 64-bitars krypterad text, [1] (se Figur 2.11).



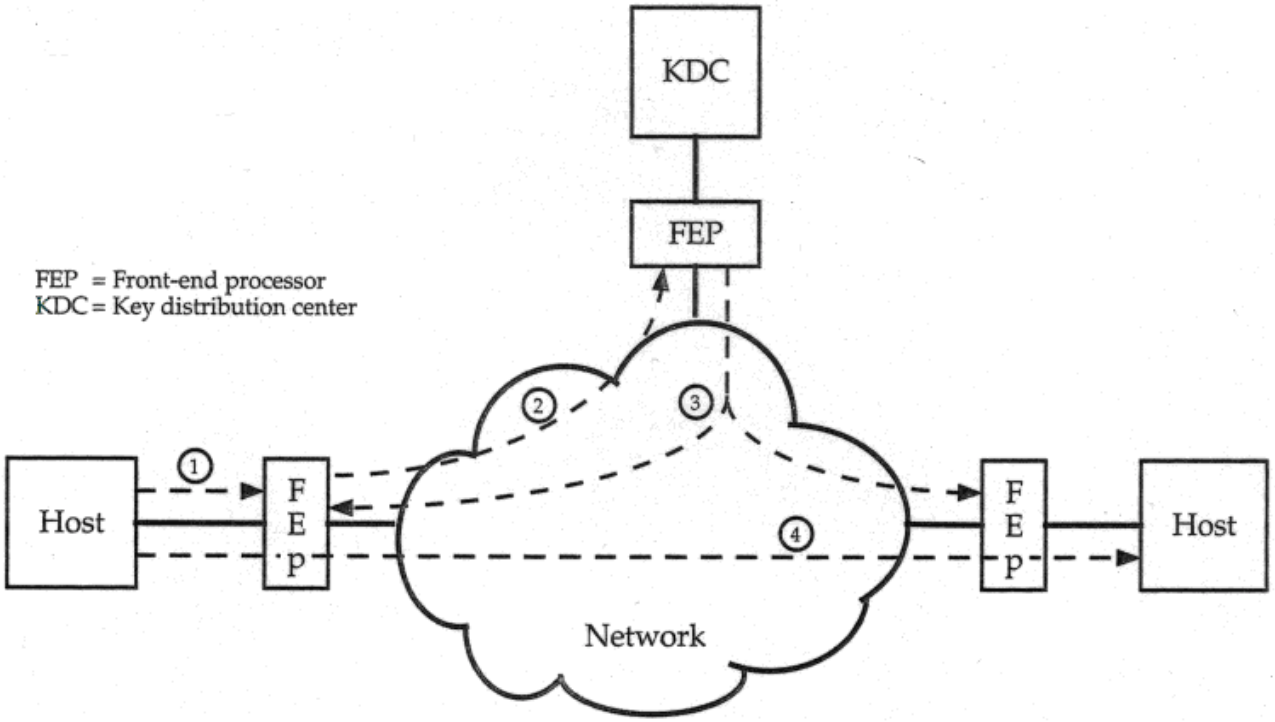
Figur 2.11 IDEA, [1].

IDEA är svår att knäcka, för det finns 2^{128} olika kombinationer att kontrollera. Först måste man få fram ett meddelande och sedan se om det verkar rimligt. IDEA är däremot inte lika beprövad som DES. Det bästa är att ha en algoritm som är välprövad, så att de flesta kryphål etc. har hittats och åtgärdats och att det inte är trivialt att knäcka nyckeln.

2.9.2.4 Distribuering av nycklar

Ett problem med kryptering är hur krypteringsnyckeln ska distribueras säkert till användarna. En möjlighet är att låta en kurir leverera nyckeln. Om nyckeln byts ofta eller om det är stora avstånd mellan de som behöver nyckeln, tar det mycket tid. För att lösa det kan automatisk nyckeldistribution användas. I Figur 2.12 visas ett exempel som är transparent för användaren.

1. Värddatorn (host) sänder ett paket med en uppkopplingsbegäran.
2. FEP buffrar paketet och frågar KDC om vilken sessionsnyckel som ska användas.
3. KDC distribuerar ut sessionsnyckeln till FEP enligt figur.
4. Det buffrade paketet sänds.



Figur 2.12 Automatisk nyckeldistribution, [8].

2.9.3 Certifikat

Vid asymmetrisk kryptering, är det viktigt att veta vem man får nyckeln från. RSA Digital Certificate har utvecklats för att underlätta utbyte av publika nycklar, [2]. I dagligt tal benämns det certifikat. Man kan se det som ett digitalt pass eller identitetskort. Certifikatet ska innehålla användarens publika nyckel. Den nyckeln ska vara signerad med en digital signatur av en utfärdare som motparten litar på. Certifikatet ska även innehålla vanlig information, såsom namn, organisation, postadress och förfallodatum. För att verifiera ett certifikat, används den publika nyckeln från utfärdaren av certifikatet och man kan därigenom kontrollera äktheten av certifikatet.

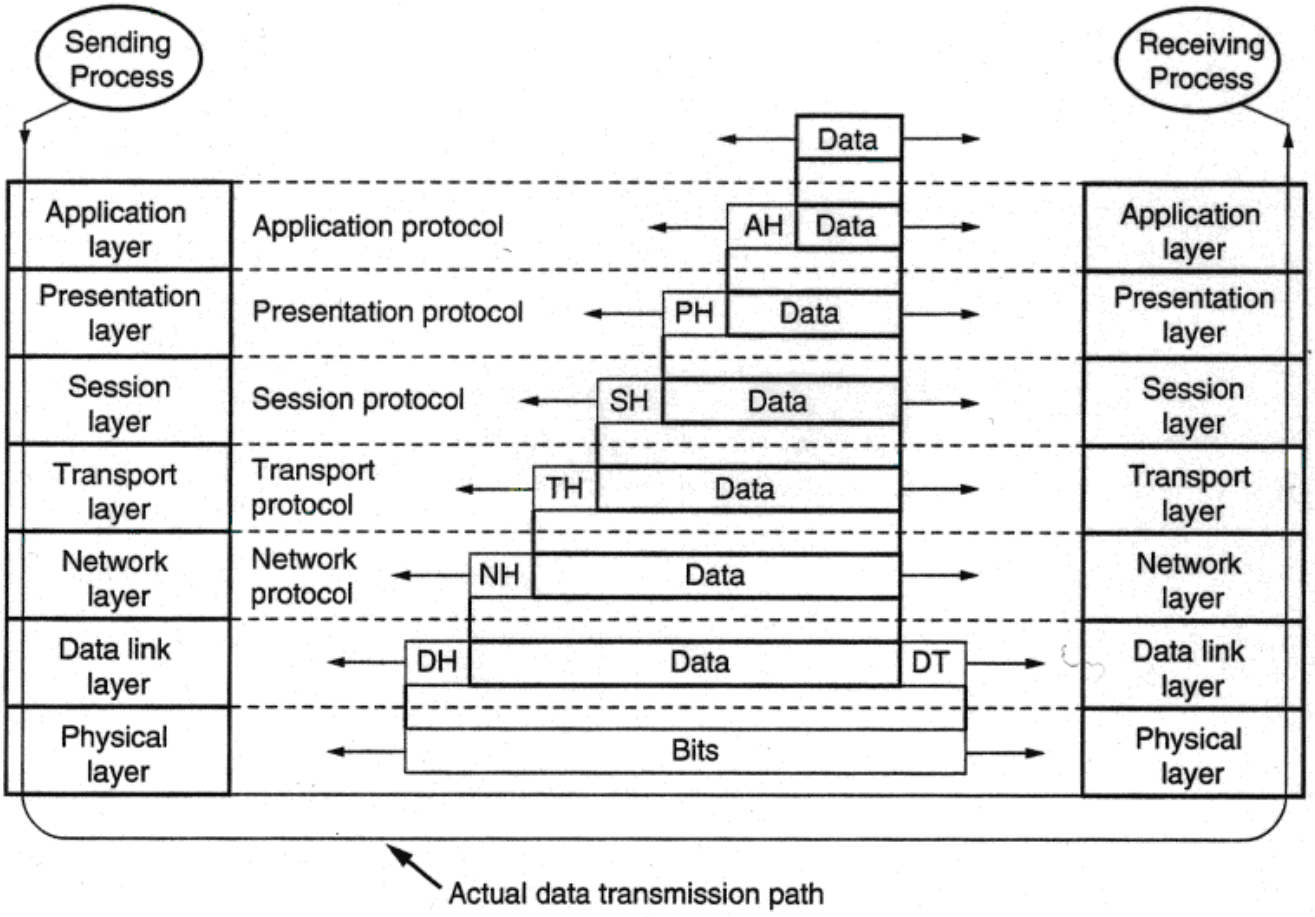
2.9.4 Checksumma

Det är fullt möjligt att någon kan ändra ett meddelande efter att det har skickats. För att kunna bevisa att det inte har förändrats på vägen kan avsändaren ta fram en s.k. checksumma på hela eller delar av det skickade meddelandet, kryptera checksumman och skicka med i meddelandet, [5]. Checksumman får man fram genom att beräkna ett värde som är beroende av hur meddelandet ser ut och är unikt för just detta meddelande. Det går alltså inte att få fram

samma checksumma på två olika meddelanden även om de är i stort sett lika. Mottagaren kan dekryptera checksumman och själv kontrollera om data har ändrats.

2.9.5 Var ska krypteringen ske?

Krypteringen kan i stort sett ske i vilket OSI-lager som helst, men de lämpligaste är fys- (physical layer), transport- (transport layer) och applikationslagret (application layer), se Figur 2.13.



Figur 2.13 OSI-modellen, [5].

På fyslagret sker krypteringen genom att en kryptobox sätts in mellan dator och sändmedium. Detta kallas link encryption. En fördel med detta är att allt krypteras, även headrarna. Det förhindrar att någon kan göra trafikanalys. Det är mest militären och företag som hanterar företagshemligheter som är känsliga för trafikanalys, men för vanlig kommersiell trafik spelar det oftast ingen roll om någon kan kontrollera var trafiken går.

Om krypteringen istället sker på transportlagret blir hela sessionen krypterad vilket ibland kan leda till en onödigt stor overhead.

Kryptering i applikationslagret gör att bara det nödvändigaste krypteras.

2.10 Attackerare

Idag innebär det en risk att skicka information över Internet. Det finns många som försöker göra intrång i datorsystem. De kallas för attackerare eller hackers. Det finns aktiva attackerare som är ute efter att försöka bryta sig in i ett system och förstöra eller stjäla information medan passiva attackerare bara är nyfikna på att se vad det är för trafik som sänds.

2.10.1 Olika typer av attacker

- För att dölja sin verkliga identitet kan man förfalska sitt IP-nummer när man gör en attack, dvs förfalska avsändaradressen i datapaketen som skickas mot målet. Det kallas IP-spoofing, som även kan användas för att få samma rättigheter som en specifik dator har genom att använda den datorns IP-nummer.
- Man kan blockera t.ex. en brandvägg eller dra ner tillgängligheten genom att bombardera den med data.
- En sniffer avlyssnar trafiken på ett IP-nät för att t.ex. få reda på lösenord eller annan data som sänds över Internet. För att skydda sig mot detta använder VPN kryptering som förhindrar att den som får tag på informationen kan förstå den.
- En attackerare som får tag på datapaket, t.ex. en betalning, som sänds över Internet kan sända om dem senare. För att förhindra detta kan man sätta en tidstämpel på paketen som talar om hur länge de är giltiga. Ett problem med detta är att klockorna i nätverket ofta inte är synkroniserade, så det kan vara svårt att avgöra om det är ett gammalt eller nytt paket.
- Om attackeraren får tillgång till ett krypterat meddelande kan en Brute force attack användas, vilket innebär att olika krypteringsnycklar testas på meddelandet tills det ser korrekt ut.

2.11 Exempel på VPN-tillämpningar

Som exempel på möjliga VPN-lösningar behandlas här vissa Internetbankers lösningar. Av säkerhetsskäl kunde de inte lämna ut information om hur serversidan ser ut.

2.11.1 Föreningssparbankens lösning

För att slippa göra sina bankärenden på bankkontoret, finns smartcarddosan med vilken man kopplar upp sig mot banken via Internet. Därifrån sköts allt från att betala räkningar till att flytta pengar mellan konton. Eftersom det är känsliga uppgifter som skickas över Internet som

t.ex. konto- och personuppgifter, så krävs det stor säkerhet som uppnås med bland annat autentisering och kryptering. För att logga in och utföra bankärenden på deras webbsida krävs en smartcarddosa. När man loggat in med smartcarddosan är man på en säker anslutning. För att öka säkerheten har de nyligen gått över från 40 till 128 bitars kryptering[6], [11].

Föreningssparbankens lösning använder sig av cockies. När en cockie har accepterats så tillåts en dialog mellan datorn och banken via Internet. Informationen i cockien används vid uppkopplingen mot deras server och för att en dialog ska kunna upprätthållas under den tid man är uppkopplad. Föreningssparbanken har ca 360 000 anslutna kunder och 24 000 inloggningar/dag, [15].

2.11.2 Skandiabankens lösning

För att kunna använda Skandiabankens banklösning över Internet, måste datorn vara inställd på att acceptera cockies. Deras VPN-lösning bygger på att man får ladda hem ett personligt certifikat (cockie). Certifikatet får man genom att klicka på fliken ”Hämta certifikat” och sedan följa instruktionerna. Certifikatet gör att Internetbanken vet att det verkligen är rätt person som försöker koppla upp sig och kommunicera med banken. Varje person ska ha ett certifikat per dator. Sedan är det bara att gå in på www.skandiabanken.se och klicka på ”Logga in” där man skriver in personnummer och en personlig PIN-kod. Även om man har flera olika certifikat så använder man sig av samma PIN-kod. Det kan jämföras med en bankomatkod där man har samma kod till alla uttagsautomater. Skandiabankens VPN-lösning använder sig av 128-bitars kryptering. De har inte haft några intrångsförsök eller andra problem. Idag har de totalt cirka 330 000 kunder, och ca 70 000 av dem använder sig av Internetbanken. De har ca 700 000 inloggningar per månad, [12].

2.11.3 Handelsbankens lösning

Liksom Skandiabanken använder sig även Handelsbankens Internetlösning av certifikat. För att använda Internet till att göra sina bankärenden på Handelsbanken måste man först ladda ner ett säkerhetsprogram till sin egen dator och välja ett lösenord som måste bestå av minst fyra bokstäver och två siffror. Det får inte innehålla delar av certifikatnamnet eller personnumret och inte tre lika tecken efter varandra. Man kan bara ha ett fungerande certifikat per personnummer, men det certifikatet kan kopieras till olika datorer. Det behövs för att man ska kunna identifiera sig och underteckna olika transaktioner. Om man t.ex. ska betala en

[6] Det kan ställa till problem, då vissa gamla webbläsare inte ställs om automatiskt. Då kan det vara lämpligt att ladda ner en gratis webbläsare från Internet.

räkning så får man signera den innan pengarna dras från kontot. Signeringen görs med lösenordet. För att ingen utomstående ska kunna se vad som skickas så krypteras alla meddelanden över den säkra förbindelsen medan man är inloggad mot banken med 128 bitars 3DES, [13]. De använder cockies till en rad ändamål, bland annat för att hålla reda på vilket bankkontor kunden tillhör och om kunden är på- eller avloggad. Certifikatet innehåller en öppen del med information om kundens personnummer, certifikatets giltighetstid och den publika nyckeln. Det innehåller även en krypterad del som innehåller den privata nyckeln. Nyckeln är krypterad med 3DES med det hashade lösenordet som krypteringsnyckel. Man lagrar alltså inte själva lösenordet på sin dator, och inte heller på banken eftersom den privata nyckeln aldrig lämnar klientdatorn. Det enda som lagras är den privata nyckeln som är krypterad med lösenordet. Man måste använda den privata nyckeln vid inloggning och signering. För att kunna göra det måste den dekrypteras, och enda sättet att göra det är att mata in lösenordet så att dekrypteringsalgoritmen kan köras så man får ut den privata nyckeln i läsbar form. Handelsbanken har ca 250 000 kunder.

2.12 Program över Internet

Om man behöver köra client/server-baserad eller webbaserad programvara måste VPN-lösningen kompletteras, liksom vid andra fjärrarbetslösningar, med en applikationsserver som t.ex. Microsoft Terminal Server eller Citrix som använder sig av tunna klienter, [2]. Det kan t.ex. vara aktuellt för distriktssköterskor som behöver komma åt patienters journaler med VPN.

Tunna klienter är samlingsnamnet på enheter med begränsat operativsystem, som används som terminaler till större system. Med tunna klienter flyttas all applikationslogik, det som utför själva databehandlingen och beräkningen, till servern. Med tunna klienter i nätverket blir det enklare att administrera, eftersom det räcker att installera programvaran i servern istället för på varje klient. Den klient som nämns oftast när man beskriver tunna klienter är webbläsaren.

2.12.1 Microsoft Windows NT4 Terminal Server Edition

WTS (Microsoft Windows Terminal Server) är ett system som använder sig av tunna klienter, vilket innebär att nätverket har en central server där alla applikationer ligger lagrade, [7]. Sedan använder man vanliga PC-enheter som terminaler till servern. Detta innebär att alla applikationer, även operativsystemet, körs centralt på servern. Man kan även installera en Terminal Server klient på en PC som redan har ett eget operativsystem och andra program på

sin hårddisk. En variant är att låta Officepaketet ligga lokalt på varje dator, och låta stora verksamhetssystem som har många användare ligga centralt på WTS-servern. Fördelar med detta är att man sparar diskutrymme på varje PC då man bara behöver installera de stora systemen på ett ställe, det är också lättare att sköta drift och underhåll. Det enda som skickas över nätverket är tangentbords-, mushanterings- och skärmbildsinformation. Alla tunga processer körs hela tiden internt på servern och belastar inte nätet. En nackdel med att ha programvaran på servern är att om servern går ner så fungerar inte någon av de terminaler som kör mot servern, förutsatt att de inte jobbar med program som finns lokalt på deras maskiner.

2.12.2 Citrix

Citrix Winframes är ett konkurrerande serversystem till WTS. Winframe erbjöd en fleranvändarversion av Windows NT, som fungerar ungefär som Terminal Server, fast den baserades på Windows NT server 3.51. Här behövs förutom programvaran till själva servern också ett klientprogram. Citrix Winframes gjorde att Microsoft fick upp ögonen för en terminalserver och konstruerade WTS.

2.13 Positivt/negativt med VPN

Eftersom det finns ett stort behov av ökad säkerhet använder sig idag många företag av VPN, och de flesta är mycket nöjda. Tidningen ”Säkerhet & Sekretess” bedömning av VPN är: ”Flexibiliteten, den låga kostnaden och framtidssäkerheten talar för att det kommer att slå igenom som det enda vettiga sättet att kommunicera.”, [2].

Ett användningsområde för VPN är att koppla ihop olika arbetsplatser med varandra. Det kan behövas om företaget är utspritt på en stor geografisk yta. Det är flexibelt då man kan välja mellan vanlig modemanknytning, ISDN eller fast lina ute på de olika arbetsplatserna. Man kan ha olika lösningar beroende på ekonomi, antal medarbetare och behov av bandbredd. Med VPN kan man koppla upp sig till en Internetleverantör mot lokal taxa eller 020-nummer. När man ringer till ett 020-nummer betalar man bara en markering själv[7], [2].

[7] Ett problem är dock att skattemyndigheten har beslutat att företag inte får betala Internetabonnemang åt sina anställda utan att också betala sociala avgifter på summan och dra inkomstskatt för värdet åt den anställde. Därför är det inte så attraktivt att göra det. Undantaget till regeln är om datorn ska användas mestadels i arbetet, för då är det inte skattepliktigt [2].

VPN är billigt jämfört med många andra lösningar. En anledning till det är att datorer, modem och Internetkoppling oftast redan finns. Kostnad för bl.a. VPN-server kan tillkomma.

Om man inte har VPN utan tar med sig filer hem från jobbet på diskett eller via mail för att arbeta med, så kan det bli versionsproblem, dvs man är inte säker på om man jobbar med den senaste versionen eller inte. Med VPN kan man arbeta mot den riktiga filen på jobbet hela tiden. Om man inte har fast uppkoppling kan man spara ner filen på sin hårddisk då det kan bli dyrt att sitta uppkopplad hela tiden man jobbar med filen. Man får då göra det till en rutin att alltid spara tillbaka filen till jobbet när man är klar, men då har man inte löst versionsproblemet. Om man skulle komma på att man har glömt den nyaste versionen hemma, så går det inte att gå bakvägen, dvs gå från jobbet via VPN och hämta data på sin hemdator.

3 VPN och nätverkssäkerhet hos Karlstads kommun

Detta examensarbete om Karlstads kommuns IT-enhet är en utredning om hur VPN skulle kunna fungera i deras verksamhet. Rapporten undersöker hur det ser ut idag, deras framtidsvisioner och avslutas med en beskrivning av en lämplig VPN-lösning. För att få en inblick i Karlstads kommuns användning av datorer och kunskap om datasäkerhet skickades en enkät ut till 40 IT-ansvariga inom Karlstads kommun (se bilaga B).

3.1 IT-säkerhet vid Karlstads kommun

I Karlstads kommun finns det IT-ansvariga på de olika förvaltningarna och ytterst ansvarig för IT/data-frågor är IT-enheten. Idag har alla ett eget lösenord för att kunna logga in i datorn och för att komma åt mailen. Från enkät och intervjuer har framkommit att det är mycket olika mellan avdelningarna och olika anställda hur stor datorvana de har, och hur ofta datorer används i arbetet. Vissa hanterar ofta sekretessbelagd information medan andra i stort sett aldrig gör det. Det skickas även arbetsmaterial som är under bearbetning. Vissa använder sig sällan av att skicka mail, andra gör det ofta. Det verkar inte vara vanligt att man skickar känsliga uppgifter via mail, trots att man inte är medveten om riskerna. Även om det inte är sekretessbelagd information, så kan informationen vara känslig och ha med den personliga integriteten att göra.

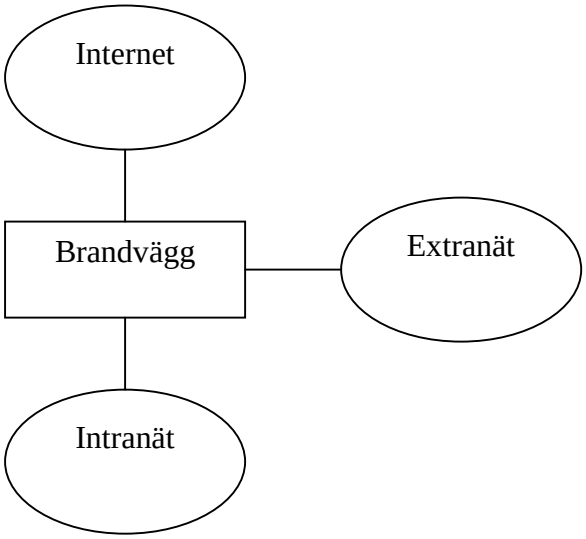
Från enkäten framkom även att många har efterlyst möjligheten att komma åt mail och intranät via Internet. Idag förekommer det att man skickar hem filer från arbetet till sin privata mailadress.

Ett alternativ till att sitta kvar på jobbet på övertid kan vara VPN. Då kan arbetet utföras hemma med full tillgång till alla dokument på jobbet. Men Karlstads kommun har regler för vilka som får distansarbeta, så detta kommer inte att medföra att alla kan börja jobba hemifrån.

Gemensamt för flera förvaltningar är att de någon gång per månad skickar sekretessbelagd information till sina programvaruleverantörer, som t.ex. vid utredning av systemfel i deras verksamhetssystem, eller skickar en integrationsfil med olika typer av totalposter till ett annat system för test.

3.1.1 Karlstads kommuns brandvägg

Karlstads kommun har sin brandvägg i en UNIX-dator (med AIX-operativsystem). Den har 4 nätverkskort, men bara 3 används idag, se Figur 3.1. De har ett nätverkskort mot intranät, ett mot extranät och ett mot Internet.



Figur 3.1 Strukturen över Karlstads kommuns brandvägg och anslutna nät.

På intranätet ligger alla administrativt anställda inom kommunen (karlstad.se). Lärare och elever är anslutna till Internet, och på extranätet ligger mail och andra resurser som de får tillgång till (t.ex. www.tingvalla.karlstad.se). Man har fler öppningar från Internet mot extranätet jämfört med mot intranätet, för att få bättre säkerhet. Det betyder att man får göra mer från Internet mot extranätet än vad man får göra mot intranätet.

Programvaran i brandväggen är IBM firewall 3.1. Den släpper bara igenom TCP/IP-trafik. Den kontrollerar ip-paketens destinationsport mm för att se om det den vill göra är tillåtet eller ej. Om en dator med ett visst IP-nr t.ex. vill använda Telnet för att ansluta sig mot en annan server så kontrollerar brandväggen om det är tillåtet.

Webbservern är en cashande webbproxy. Den gör en förbindelse från en PC i intranätet till brandväggen, där gör den en ny förbindelse från brandväggen till Internet och går och hämtar det den ska hämta, sedan ger den det till den interna förbindelsen som frågade efter det. Man går alltså inte rakt igenom. Att den är cashande innebär att brandväggen lagrar de sidor den nyligen hämtat, så om någon senare vill hämta samma sida räcker det att bara gå till brandväggen. Brandväggen kan även ta emot ett ftp-anrop från webbproxyn och sedan göra om det till ett riktigt ftp-anrop. Men det finns även en speciell proxy som bara har hand om ftp som heter ftp-proxy, och fungerar ungefär som webbproxyn med skillnaden att inloggning krävs.

På intranätet använder man privata 10.10.x.x adresser, men det går inte att använda dem när man t.ex. vill använda Telnet för att koppla sig till en annan server, för då krävs en riktig IP-adress. I brandväggen ligger en pool med 256 olika adresser, NAT-poolen. NAT står för Network Adress Translation. Där tar man en ny registrerad adress. När man har fått en adress så är den upptagen och ingen annan kan ta den. Man översätter bara adressen när man går rakt igenom brandväggen annars när man t.ex. har delat upp anropet i brandväggen så använder den brandväggens egen IP-adress som alltid är samma. Anropen delas upp när det är proxyanslutningar, men inte vid t.ex. Telnet som går rakt genom. Att använda sig av adressöversättning med NAT hindrar att någon på t.ex. Internet kan få reda på varje dators interna ip-adress och hur strukturen ser ut på intranätet.

Mail använder sig av SMTP för att skicka mail och POP3 för att hämta mail. I intranätet finns en mailserver: postoffice = ”Pilen” som har både SMTP och POP3 för att kunna skicka/ta emot mail. Detsamma gäller extranätets mailserver: mailbox = ”Boken”. Men brandväggen däremot har bara SMTP, för den bara skickar vidare mailen dit den ska utan att titta på den, så den behöver inte hämta mail, utan bara skicka vidare.

Vissa leverantörer får ansluta sig via extranätet och därifrån gå vidare genom brandväggen till intranätet, t.ex. till en viss dator där. Anledningen till att de får anslutas till extranätet är att om de ansluter sig direkt från Internet så är det lätt att någon fejkar avsändaradress och kan komma åt intranätet. Om leverantörerna istället får ansluta direkt mot intranätet, så är det svårt att kontrollera vad de får göra och vad de gör. Det bästa är därför att låta dem komma via extranätet.

Det finns en inbyggd VPN-lösning i IBM FW 3.1. En nackdel med brandväggen är att den använder 56 bitars DES-kryptering, men i nyare versioner används istället 3DES som är säkrare, [3]. IBM FW 3.1 stödjer IPSec.

3.1.2 Scenarion för Karlstads kommun

Om Karlstads kommun bestämmer sig för att låta alla få tillgång till enbart mail via VPN, så är det lätt att administrera. Det är alltid enklast om alla har samma rättigheter, men när det gäller Karlstads kommun så kan man räkna med att det kommer att bli flera grupper med olika rättigheter och därmed svårare att organisera och administrera. För att kunna arbeta hemifrån vill de anställda ha möjlighet att få tillgång till både mail och filer. Om det bara är ett fåtal förvaltningar som kommer att få tillgång till VPN kan de få varsin smartcarddosa för att kunna logga in hemifrån.

Om de flesta på förvaltningarna skall få tillgång till VPN, blir det dyrt att köpa in smartcarddosor till alla. Då kan istället teknikansvariga eller chefer på varje förvaltning ta fram och dela ut lösenord för att kunna logga in på en VPN-lösning som liknar den som Skandiabanken använder. Om Handelsbankens lösning används där man själv väljer sitt lösenord och matar in direkt i datorn, kommer man ifrån administration av lösenord.

Skulle alla i hela Karlstads kommun få tillgång till VPN kan det vara lämpligt att välja olika lösningar för olika förvaltningar. För personer som reser mycket i tjänsten kan det vara bra med en smartcarddosa som kan användas på vilken dator som helst utan att behöva ladda ner ett certifikat, eller lägga in en mjukvara från diskett/CD-skiva. Om det däremot är en person som i stort sett alltid sitter vid samma dator är det bättre att ha endera en mjukvara på varje klientdator, eller använda Handelsbankens lösning där man laddar ner ett certifikat. Det är säkrare att använda en smartcarddosa än ett certifikat, även om certifikatet är mer praktiskt, [2]. Filer på en hårddisk kan återskapas långt efter att de tagits bort. Detsamma gäller även för certifikatet. Karlstads kommun hanterar en del känslig information, och därför är det bäst att alla får en smartcarddosa.

3.1.3 VPN på intranätet eller bara på Internet

För att informationen ska skyddas även internt måste VPN finnas även på intranätet. Man får ställa sig frågan om det är nödvändigt att skydda informationen internt inom Karlstads Kommun, eller om det räcker att inte utomstående kan komma åt den, [2].

3.2 Servrar/arkitektur

Karlstads kommun har samlat sina servrar på IT-enheten, där all trafik till och från dem måste gå genom den befintliga brandväggen. En VPN-server kan placeras vid brandväggen eftersom all trafik passerar där. Klienter får distribueras ut till de användare som ska ha tillgång till informationen.

3.3 Säkerhetspolicy

Vilka som kommer att få tillgång till VPN och när, kommer att beslutas vid senare tillfälle.

Det kan vara bra att börja med VPN på en förvaltning för utvärdering och sedan gå vidare tills alla har tillgång till det. Om alla istället får tillgång till VPN samtidigt kan det bli problem, särskilt för supporten. För att underlätta för supporten kan det vara bra att ha en FAQ på nätet med de vanligast ställda frågorna, där de anställda i första hand ska gå in och

läsa. Om de inte blir hjälpta av det kan de ringa supporten. Det kan vara bra att ha en log för att se vilka som har gjort vad och när. Det bör specificeras hur mycket man får titta i loggen. Samma säkerhetspolicy bör gälla både för uppkoppling direkt mot intranätet eller via VPN.

3.4 Alternativ lösning utan VPN

Inom Karlstads kommun har inte alla behov av VPN, utan det skulle räcka att flytta ut intranätet (Solsidan) på Internet och skydda sidorna med ett password, och låta alla få en mailadress av typen Hotmail som man kan komma åt från valfri dator med Internetuppkoppling. Denna lösning skulle vara lämplig för t.ex. alla skolelever i kommunen. Idag ligger samma information på flera ställen, både på Internet och på intranätet, t.ex. namn på anställda på olika enheter. Det skulle man komma ifrån om man flyttade allt till Internet. Med denna lösning kan man inte komma åt intranätets filer hemifrån.

3.5 Rekommendationer för Karlstads kommun

De anställda inom Karlstads kommun anser att det är viktigt att kunna få tillgång till intranätet som mail, filer mm hemifrån. För att lösa detta på ett säkert sätt, finns behov av en VPN-lösning. Det bästa alternativet för Karlstads kommun är en blandning av en brandväggsbaserad och mjukvarubaserad lösning där VPN-servern ligger bakom brandväggen och en port för VPN-trafik öppnats (se punkt 2.5.2, 2.5.3 och 2.5.4). Anledningen till att öppna en port är att man slipper konfigurera ett filter i brandväggen som låter VPN-trafik passera. Filtreringen sker istället i VPN-serverns mjukvara där all VPN-trafik hanteras men andra typer av paket kastas. Mjukvarubaserad VPN-server innebär att man kan definiera olika starkt krypterade tunnlar till olika destinationer, baserat på adress eller protokoll. Trafik som inte kommer in på VPN-porten hanteras av den befintliga brandväggen.

Varje anställd får en smartcarddosa som ger möjlighet att logga in i Karlstads kommuns intranät även om man befinner sig utanför brandväggen (se punkt 2.5.6). För att minimera risken att någon obehörig ska komma åt intranätet, kan man ha automatisk utloggning från VPN-applikationen om man varit inaktiv i t.ex. 20 min. Man kan även ha automatisk utloggning från smartcarddosan efter t.ex. 1 min.

Anledningen till att lösningen valts är att det är smidigare att ge varje anställd en smartcarddosa för autentisering, än att distribuera ut en programvara och se till att den installeras och konfigureras korrekt hos klienterna. Man kan dessutom logga in på Karlstads

kommuns intranät med smartcarddosan från vilken dator som helst, förutsatt att den har en Internetuppkoppling.

Med denna typ av lösning går användaren till en Internetsida där han autentiserar sig med smartcarddosan. VPN-servern identifierar användaren, och en tunnel sätts upp mellan dem.
Det vore lämpligt att använda sig av 128 bitars kryptering.

Krypteringen ska vara så säker att den klarar sig inom den närmaste framtiden. Man kan ha ett program som gör om krypteringsnycklarna automatiskt med jämna mellanrum för att förhindra att dokument som ska sparas en längre tid är krypterade med en nyckel som är knäckt. VPN-lösningen bör vara standardprodukt. Alla som har tillgång till VPN ska kunna använda det.

Det finns flera olika alternativ till hur man ska hantera användarnas utbildning på VPN. En fråga i enkäten handlade om utbildning. Resultatet var att den utbildningsmetod som de flesta, 43 %, inom Karlstads kommun ansåg bäst var användarmanual.

Man kan ha olika utbildning för olika förvaltningar, beroende på hur stor datorvana de anställda har. För många skulle en vanlig användarmanual räcka, men för andra skulle det vara svårt att inte ha någon som visar hur man ska göra. Det kan resultera i att VPN inte kommer att användas.

3.6 Att tänka på vid val av leverantör

Idag finns det många olika leverantörer att välja bland. I stort sett varje leverantör av brandväggar, modem och switchar har en egen VPN-lösning.

Karlstads kommun använder helst standardprodukter. Det finns flera viktiga aspekter att tänka på när man ska välja leverantör, [2]. Man behöver inte välja en VPN-lösning från den leverantör man har köpt från tidigare. De flesta VPN-lösningarna stödjer IPSec, och då är kompatibiliteten bra så de olika säkerhetsprodukterna kan kommunicera med varandra även om de kommer från olika leverantörer. Med vissa VPN-lösningar kan det bli problem om tunneln används mer än 24 timmar, [14].

3.6.1 Pris

En viktig fråga är hur mycket man är beredd att betala för sin VPN-lösning. Det kan skilja mellan olika leverantörer. Om en VPN-lösning stämmer bra in på de krav som satts upp, men är för dyr, får man endera vara beredd att betala mer än man tänkt sig från början eller ta bort vissa funktioner i VPN-lösningen för att få det lite billigare. Det gäller att hitta en balans mellan pris och innehåll.

3.6.2 Support 18.00 – 07.00

Om det är viktigt med support mellan 18.00 – 07.00 och på helger är olika för olika förvaltningar beroende på hur deras arbete ser ut.

Från enkät framkom att för de flesta, 62 %, var det inte viktigt med support, utan det kan räcka att någon har telefonjour varje dag. Om IT-enheten ska stå för den supporten blir det en extra arbetsbörda för dem, så varje förvaltning kan stå för sin egen support istället. Oftast går det bra att vänta till dagen efter och fråga supporten då.

3.6.3 Krypteringsgrad

Hur stark krypteringen bör vara beror på hur viktigt det är att skydda sin information. En 64 bitars nyckel räcker för att hålla nybörjare ute, men för mer avancerade attackerare krävs minst 156 bitar. Det är svårare att lösa en lång nyckel, men det är också jobbigare för datorn att räkna ut vilken ursprungstexten var. Tidigare hade USA hårda regler för hur stark kryptering de kunde exportera, så då var 64 bitars kryptering standard, men nu har de släppt lite på sina exportregler, så det kan vara lämpligt att använda 156 bitar. Eftersom vissa förvaltningar på Karlstads kommun hanterar personuppgifter som är känsliga för att komma ut skulle 156 bitars 3DES kryptering vara lämpligt. För att kompensera en svag kryptering kan man byta krypteringsnyckel ofta, men man bör inte satsa på minde än 128 bitar om man har information man vill hålla hemlig.

En annan fråga att ta ställning till är hur mycket som ska krypteras. Om man krypterar hela meddelanden tar det längre tid än om man bara krypterar en checksumma. Om det är något som bara behöver skyddas ett tag krävs det inte så stark kryptering, men är det riktigt sekretessbelagda handlingar så är det bra med stark kryptering. Man skulle kunna ha olika stark kryptering beroende på hur viktigt det är att skydda. Det skulle kunna baseras på t.ex. IP-adresser.

4 Slutsats

Den här studien har kommit fram till att eftersom de flesta anställda i Karlstads kommun efterfrågar möjligheten att kunna komma åt intranätet med mail och filer hemifrån på ett säkert sätt skulle VPN vara en bra lösning. Även om det inte går att nå 100 % säkerhet med VPN, så är VPN ett mycket bra alternativ för Karlstads kommun. Den lösning som anses bäst för en organisation som Karlstads kommun är enligt denna studie en blandning av brandväggsbaserad och mjukvarubaserad lösning där VPN-servern ligger bakom brandväggen och en port i brandväggen öppnas för VPN-trafik (se punkt 3.5). Varje anställd får en smartcarddosa som ger möjlighet att logga in i Karlstads kommuns intranät om man befinner sig utanför brandväggen. Anledningen till att den lösningen rekommenderas är att det är smidigare att ge varje anställd en smartcarddosa än att distribuera ut en programvara och se till att den installeras och konfigureras korrekt. Man kan dessutom logga in på Karlstads kommuns intranät med smartcarddosan från vilken dator som helst, som har en Internetuppkoppling.

Referenser

[1] Andrew S. Tannenbaum. *Computer Networks*, third edition. Prentice-Hall, Inc, 1996.

[2] Tidskrift: *Säkerhet & sekretess* nr 5 1999

[3] IBM:s brandvägg, http://www2.ibmlink.ibm.com/

[4] IPSec, http://www.lysator.liu.se/upplysning/990427.html

[5] Material från kurserna DatakommunikationI&II, Karlstads universitet.

[6] Introduktion till hemliga och öppna nyckar,
http://www.webway.se/intranetica/kds/nycklar.shtm

[7] *Utredning om Windows NT4.0 Terminal server*, Per Andreasson

[8] William Stallings, *Network and Internetwork Security Principles and Practice*, Prentice Hall, 1995.

[9] Digitala signaturer, http://www.intranetica.com/intranetica/kds/

[10] Kryptering, http://www.intranetica.com/intranetica/kds/krypto.shtml

[11] Föreningssparbankens Internetbanklösning, http://www.foreningssparbanken.se/

[12] Skandiabankens Internetbanklösning, http://www.skandiabanken.se/

[13] Handelsbankens Internetbanklösning,
http://www.handelsbanken.se/hemsidor.nsf/kontorsval/nystartsidany

[14] Joel Snyder, Securing the last mile, Network World, 12/13, 1999, http://www.nwfusion.com/reviews/1213vpnrev.html

[15] Frederic J. Cooper, Chris Goggans, *Implementing Internet Security*, New Riders Publishing, 1995.

[16] The development of network security technologies,
http://www.smartsec.se/faq/fwhist-wp.htm

A Bilaga ordlista

DES	Data Encryption Standard.
3DES	Trippel DES.
FAQ	Frequently Asked Questions.
ftp	File Transfer Protocol.
FEP	Front-End Processor.
FW	Firewall, brandvägg.
IDEA	International Data Encryption Algorithm.
IP	Internet Protocol.
IPSec	IP Security Protocol.
IPv4	Internet Protocol version 4
ISDN	Integrated Services Digital Network.
ISP	Internet Service Provider, Internetleverantör.
KDC	Key Distribution Center.
NAT	Network Address Translation.
OSI	Open Systems Interconnection.
PKI	Public Key Infrastructure.
POP3	Post Office Protocol-3.
RSA	Rivest, Shamir, Adleman Digital Certificate.
SMTP	Simple Mail Transfer protocol.
VPN	Virtuella Privata Nät.
WTS	Microsoft Windows Terminal Server.

B Bilaga Enkät

Frågor:

1. Använder Ni Er av att skicka information via Internet idag, t.ex. filer via e-post? (J/N):
Ja: 100%
Nej: 0%

2. Brukar Ni skicka personuppgifter eller annan sekretessbelagd information? Markera lämpligt alternativ med ett kryss, x:

( ) nästan aldrig: 66%
( ) någon gång per månad: 10%
( ) någon gång per vecka: 19%
( ) flera gånger varje dag: 5%

3. Skulle Ni ha nytta av att kunna skicka e-post som ingen utomstående kan läsa? (J/N):
Ja: 86%
Nej: 14%

4. Är Ni nöjda med hur det fungerar idag? (J/N):
Ja: 62%
Nej: 19%
Vet inte: . . .19%

5. Har alla på Er avdelning, på jobbet, tillgång till en dator? (J/N)
Ja: 86%
Nej: 9%
Nästan: 5%

6. Använder de sig av datorn i det dagliga arbetet? (J/N)

Ja: 95%

Nej: 5%

Använder de sig av Internet? (J/N)

Ja: 90%

Nej: 10%

7. Är det någon som arbetar hemifrån/på distans på Er avdelning? (J/N)

Ja: 62%

Nej: 28%

Inget svar: . 10%

Brukar de skicka sekretessbelagda filer eller personuppgifter hem till sina privata e-postadresser över Internet för att arbeta med? (J/N)

Ja: 24%

Nej: 52%

Vet ej: 24%

8. Är det viktigt att kunna kontrollera att ett meddelande inte har förändrats sedan det skickades? (J/N)

Ja: 90%

Nej: 5%

Sällan: 5%

9. Är det viktigt att i efterhand kunna bevisa att ett meddelande verkligen kommer från den som säger sig ha skrivit det? (J/N)

Ja: 85%

Nej: 5%

Vet ej: 10%

10. Är det viktigt att i efterhand kunna bevisa att ett meddelande verkligen kommer från Er? (J/N):

Ja: 85%

Nej: 5%

Vet ej: 10%

11. Skulle Ni utnyttja möjligheten att komma åt intranät via Internet? (J/N)

Ja: 100%

Nej: 0%

12. Om man skulle ge Er möjlighet att komma åt kommunens intranät via Internet t.ex. hemifrån, hur skulle Ni då helst vilja få utbildning på det? Markera lämpligt alternativ med ett kryss, x:

( ) utbildning behövs inte : 24%

( ) bruksanvisning/användarmanual: 43%

( ) halvdagskurs för alla: 14%

( ) kurs för en anställd som sedan berättar för de andra:23%

( ) annat förslag, nämligen 1 tim kurs: 5%

inget svar: 5%

13. Är det viktigt för Er att ha support före kl. 07.00, efter kl. 18.00 och på helger? (J/N):

Ja: 33%

Nej: 62%

Inget svar: . . 5%

14. Kommer många hos Er att arbeta efter kl. 18.00? (J/N)

Ja: 43%

Nej: 47%

Inget svar: . .10%

15. Skulle alla på Er avdelning få tillgång till att komma åt intranät från Internet? (J/N)

Ja: 65%

Nej: 30%

Inget svar: . 5%

16. Tror Ni att Ni kommer att använda Er av möjligheten att komma åt intranät från Internet i framtiden om den finns? (J/N)

Ja: 70%

Nej: 0%

Inget svar: . 30%

17. Vad skulle Ni vilja kunna göra från Internet? Markera lämpligt alternativ med ett kryss, x:

( ) titta på solsidan: 43%

( ) läsa e-post: 100%

( ) skicka/öppna filer: 90%

( ) annat: 24%

Tack för att Ni tog Er tid att fylla i frågeformuläret. Det kommer att hjälpa mig och IT-enheten mycket i det fortsatta arbetet!

Skicka frågeformuläret till mig via e-post eller under mitt namn och Karlstads kommun, IT-enheten senast 14/4.

Med vänliga hälsningar:

Charlotta Lagerkvist

Charlotta Lagerkvist
charlotta.lagerkvist@karlstad.se