Implementing a virtual private network

JOAKIM SAMUELSSON
and
RICHARD SANDSUND

KTH Information and
Communication Technology

Bachelor of Science Thesis
Stockholm, Sweden 2007

COS/CCS 2007-30

Implementing a virtual private network

Joakim Samuelsson
Richard Sandsund

Stockholm, Sweden
7 December 2007

Supervisor: Patrik Brising, Confidence

Examiner: Professor Gerald Q. Maguire Jr., KTH

Sammanfattning

Dagens företag vill ge anställda möjlighet att jobba hemifrån eller på resande fot. En vanlig lösning för att möjliggöra detta är virtual private network (VPN). VPN ger en användare tillgång till interna resurser på företaget från ett externt nät, exempelvis via Internet. Detta gör att användare kan komma åt de interna resurserna på ett säkert sätt. Vilken VPN-teknik är då att föredra för att få en så snabb, säker och pålitlig anslutning som möjligt? Detta examensarbete tar upp olika VPN-tekniker.

Vi beskriver vanliga VPN-protokoll som L2TP, IPSec och PPTP. Hur användare autentiseras på ett säkert och smidigt sätt samt metoder att göra sin VPN-anslutning säker. Vi redovisar också den lösning vi har implementerat hos Confidence, för vilka arbetet utfördes. Problemen med att använda de produkter som redan fanns på företaget beskrivs. Förslag på lösningar ges för att lösa dessa problem i framtida arbeten.

Abstract

Companies of today want to give their employees the opportunity to work from home or while they travel. A common solution to accomplish this is to implement a VPN over top of the existing network. Using VPN gives the employees access to the company's local area network from outside, via the internet. The VPN provides a secure channel for these employees to connect to the local services attached to the company's network that they need to reach. Which VPN technology is most suitable to deliver a secure, fast, and reliable connection to theses employees? In this thesis examines we are taking a closer look at different VPN solutions.

We describe different VPN-protocols like L2TP, IPSec and PPTP. How to authenticate users in a secure and flexible way and also methods used to make the VPN-connection secure. Lastly we will show the solution we have implemented at the company Confidence, for whom we made the solution. The difficulties in using existing products with the company's infrastructure are described. Suggestions are offered for future work to address these problems.

Innehållsförteckning

1 Inledning

När ett företag idag vill låta sina anställda få tillgång till det interna nätverket utifrån företagets väggar är det viktigt att detta sker på ett säkert sätt. Många företag har idag personal som ofta är på resande fot eller som helt enkelt inte behöver sitta på en fast arbetsplats på ett kontor för att göra sitt jobb. När nästan all information som man arbetar med är elektronisk räcker det med att man kan få tillgång till denna där man för tillfället befinner sig. Idag har nästan alla en egen bredbandsuppkoppling vilket gör att det går snabbt att skicka och hämta information över Internet.

Likväl som det finns tjuvar ute i samhället finns det personer på Internet som försöker ta sig in i andras datorer för att stjäla information, eller bara för att förstöra. Företag har ofta ett bra skydd mot sådana intrång. De har en brandvägg som kontrollerar allt som får komma in och ut, samt uppdaterade antivirusprogram. De inför policies som reglerar vad användarna får göra och hur de skall bete sig på företagets nätverk. Man kräver ofta olika typer av autentisering av användaren för att komma åt data på det interna nätverket.

När man då börjar tillåta arbete utanför den säkra IT miljön på kontoret så uppstår vissa säkerhetsrisker, Exempelvis:

- När den anställde använder en privat dator som fler i hushållet har tillgång till kan obehöriga komma åt företagskritisk information
- Datorn kan bli stulen
- Ett osäkert hemmanätverk där datorn står, vanligt med ingen eller dålig WLAN kryptering
- Anslutande datorer kan vara osäkrade med bristande antivirus och brandväggsregler

Det finns flera sätt att ge en användare tillgång till information på ett företagsnätverk. En förutsättning är att användaren har en Internetuppkoppling. Är detta krav uppfyllt så finns det en rad metoder att använda sig av beroende på vad man har för krav på säkerhet och vilken typ av interna resurser användaren skall kunna komma åt. Några av metoderna man kan använda sig av är att:

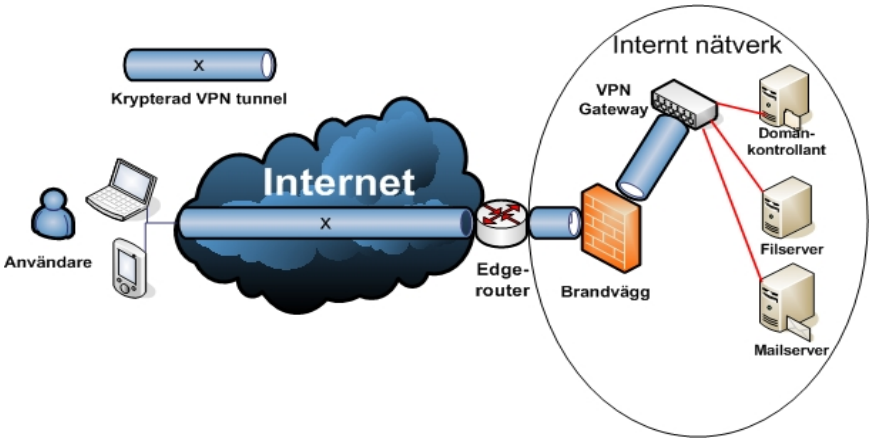
- Upprätta en File Transfer Protocol (FTP) server med den nödvändiga informationen
- Ansluta sig med remote desktop och jobba direkt på en dator inom företagets nätverk
- Ansluta sig till företagsnätet via en VPN-tunnel.

FTP är till för att föra över filer mellan en klient och en server. Detta kan vara en tillräcklig lösning i vissa fall beroende på vad användarna skall komma åt på det lokala nätverket och hur hög säkerhet man eftersträvar. Trafiken i vissa FTP-applikationer kan krypteras men då krävs stöd för Secure File Transfer Protocol (SFTP). Om användarna behöver komma åt delade mappar i företaget kan en FTP-lösning vara ett bra alternativ. FTP kan man dock

inte använda sig av i de fall användaren måste arbeta direkt mot applikationer eller andra resurser på företagets nätverk.

Att använda sig av remote-desktop är i många fall en alldeles utmärkt metod. I Microsofts lösning som kallas Terminal Services (TS) kan användaren ansluta till en server på företaget hemifrån och arbeta med filer, surfa på intranät samt arbeta med applikationer som om användaren faktiskt var på plats på företaget. Nackdelen med många remote-desktop lösningar är att det är dyra samt att säkerheten i många fall är bristfällig. Vi har framför allt testat Microsofts lösning och problemet med den är bland annat så kallade man-in-the-middle-attacks där en hackare omdirigerar trafiken och på så sätt kan lyssna på en användares knapptryckningar och då lista ut lösenord och komma åt systemet. Detta går att komma runt genom att skapa en krypterad tunnel mellan användaren och företaget som man sedan skickar remote-desktop informationen i. När en användare loggar in i Microsofts remote-desktop lösning skapas en session på terminalservern. Flera användare kan vara inloggade mot samma server med varsin egen session. Det som skickas mellan servern och klienten är grafik och knapptryckningar. Det som händer när en användare exempelvis vill öppna en fil är att filen öppnas på terminalservern och grafiken skickas till användaren som på så sätt kan läsa och arbeta med den. Detta är en skillnad mot andra distansarbeteslösningar där filerna skickas från en server till en klient, ofta över Internet.

Ett tredje sätt att tillåta användare att arbeta hemifrån är att upprätta en VPN-tunnel mot företaget. På så sätt kan man jobba med sin dator precis på samma sätt som om man satt på kontoret och var ansluten direkt till kontorsnätet. Exempel på detta visas i Figur 1 nedan.



Figur 1 Exempel på en vpn anslutning.

Tillsammans med vår handledare på Confidence kom vi ganska snabbt överens om att just VPN skulle vara den bästa lösningen för företaget. Valet stod mellan en VPN och en remote-desktop lösning och då remote-desktop kräver dyra licenser så föll valet på VPN som kan implementeras gratis med de medel som redan finns på företaget. För att implementera en VPN-lösning krävs en VPN-gateway som är en enhet som hjälper till att autentisera användarna, kryptera utgående trafik samt dekryptera inkommande trafik. Som VPN-gateway blev vårt val företagets brandvägg, en Huawei Eudemon 100. De mål som Confidence hade var att få en så användarvänlig, lättadministrerad och säker lösning som möjligt, detta skulle skapas med de resurser som fanns på företaget.

När en anställd ansluter sig till företaget så krävs det även vissa regler som talar om vilka rättigheter den anslutna användaren har. Beroende på vem det är som ansluter sig så ska de kunna ha olika rättigheter i nätverket. Vidare kommer vi att beskriva olika VPN-tekniker som finns och varför vi valde den vi implementerat, vi tar även upp andra tekniker som

använts i den färdiga lösningen. Sedan kommer en beskrivning av den färdiga lösningen tillsammans med de problem vi stött på under arbetets gång.

1.1 Övergripande Syfte

Målet med projektet är att skapa en säker VPN-tunnel och en VPN-policy åt Confidence. De anställda skall ha möjlighet att på ett säkert sätt ansluta sig till företagets nätverk utanför kontoret. Detta innefattar när de vill arbeta hemifrån, är på affärsresa, sitter hos en kund eller andra tänkbara situationer då de vill komma åt material som finns på det interna nätverket. För att göra detta möjligt krävs det att både den som vill ansluta till företaget och företaget är anslutna till Internet, som alltså är det medium vi kommunicerar över. Utöver detta krävs en så kallad VPN-gateway på företaget samt en VPN-klient hos den anställda som vill kommunicera. Vi hade tillgång till en VPN-gateway av märket Huawei Eudemon 100 på Confidence som vi använde som företagets VPN-gateway. Kravet när det gällde den andra parten i kommunikationen, VPN-klienten, var att den skulle fungera tillsammans med VPN-servern på ett så säkert sätt som möjligt. Vi skulle först och främst inrikta oss på klienter som är gratis att använda. Tillsammans med implementationen av en VPN-lösning måste även en policy för VPN-användarna i nätverket utarbetas och upprättas. Vilka rättigheter ska de anställda ha när de jobbar utifrån? Vilka nätverksenheter ska de komma åt? Vad ska de ha tillgång till? Detta är några exempel på frågeställningar att ta hänsyn till när en policy skall utarbetas.

Om vi efter att detta var klart hade tid över skulle vi även börja titta på den redan befintliga VPN tunneln mellan Confidence kontor i Göteborg och Sundbyberg. Vår uppgift här var att se om den gick att förbättra på något sätt. Användare i Göteborg upplever nämligen anslutningen som slö när de arbetar med ekonomiprogrammet Scandinavian PC Systems (SPCS). SPCS är det ekonomiprogram som Confidence använder till fakturering, orderhantering, löneadministrering och bokföring. Confidence har även kontor i England och på Irland som de skulle vilja fick tillgång till det lokala nätverket i Sundbyberg med dess resurser.

2 Bakgrundsmaterial

2.1 Översikt

VPN är en metod för att skapa säkra förbindelser över ett publikt nätverk, till exempel Internet. VPN använder autentisering och kryptering för att hålla informationen som skickas säker. VPN är ett vanligt inslag i företag där anställda behöver komma åt det interna nätet för att jobba hemifrån eller när nätverk på skilda geografiska platser behöver knytas ihop.

I VPN använder man sig av det publika Internet som transportmedel, det enda som behövs är en Internetanslutning. För att uppnå samma lösning utan att använda det publika Internet så skulle man behöva köpa eller hyra någon form av punkt till punkt anslutning vilket kan vara väldigt dyrt. I vissa fall beroende på det geografiska läget kan det till och med vara omöjligt att få tag på en sådan anslutning. Ett annat alternativ är att använda det befintliga telefonnätet men eftersom Internet både ger en högre hastighet och är billigare så är det utan tvekan den bästa lösningen i de flesta fall.

2.2 Olika VPN lösningar

En av de första aspekterna som du måste ta hänsyn till när du implementerar en VPN-lösning är mellan vilka enheter den ”säkra tunneln” skall gå. Det finns flera möjligheter och beslutet skall fattas beroende på var man vill att tunnelns ändpunkt skall vara. Man bör också vara medveten om att oavsett vilken enhet man väljer så kräver hantering av VPN-anslutningar datorkraft. En enhet med för svag datorkraft kommer att bidra till dålig prestanda och längre väntetider. I företag och andra organisationer används ofta en enhet som sköter VPN-anslutningen, att kommunikationen krypteras är ofta transparent för användaren. Till exempel så kanske VPN-enheten har ett filter som säger att den skall kryptera all trafik som ska till en viss IP-adress. Nedan beskriver vi olika enheter som kan användas som ändpunkter i en VPN-lösning.

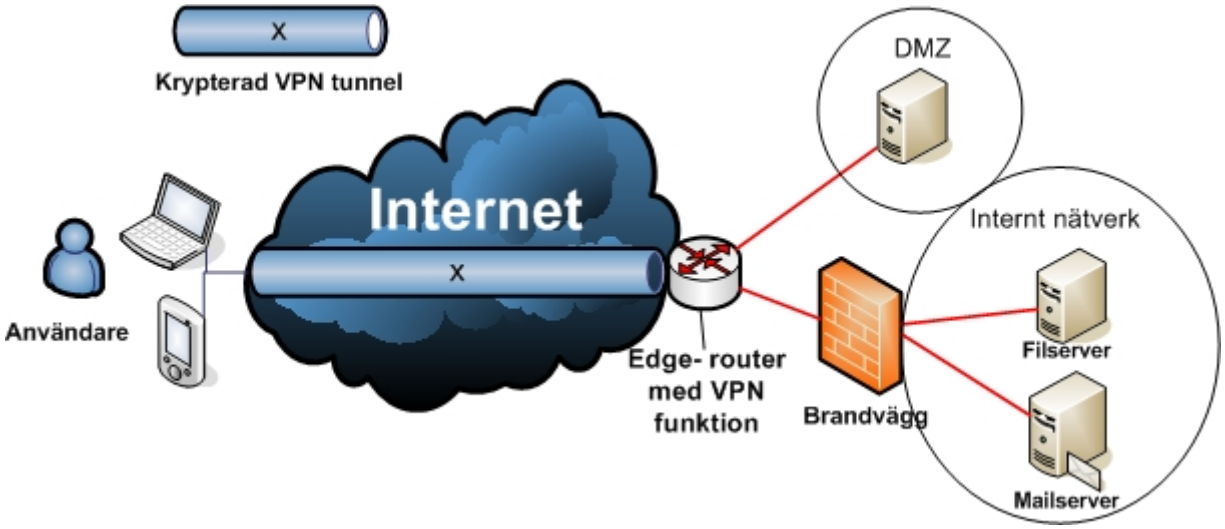
- Routerbaserad VPN-gateway
- Brandväggsbaserad VPN-gateway
- Serverbaserad VPN-gateway
- VPN-klient

Alla har sina fördelar och nackdelar, därför är det viktigt att tänka igenom vilken lösning som passar bäst för varje situation.

2.2.1 Routerbaserad VPN-gateway

Detta är kanske den mest ovanliga av de olika lösningarna men den förekommer. Denna lösning innebär att den säkra tunneln sätts upp till ett företags edge-router. Detta innebär att all VPN-trafik måste anpassa sig efter brandväggsreglerna för att komma in på det interna nätverket. Eftersom företag och andra organisationer inte gärna öppnar portar in till

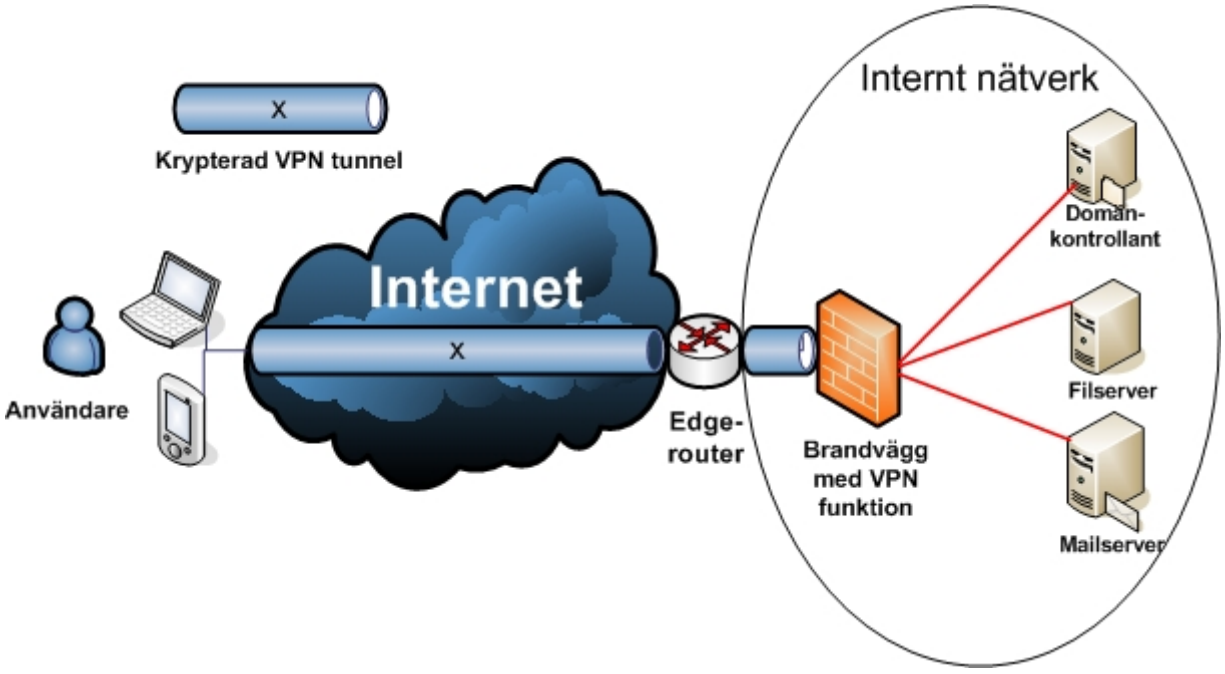
nätverket så lämpar sig den lösningen bäst för så kallade extranet. Alltså åtkomst till server i De Militarized Zone (DMZ).



Figur 2 Exempel på routerbaserad VPN anslutning

2.2.2 Brandväggsbaserad VPN-gateway

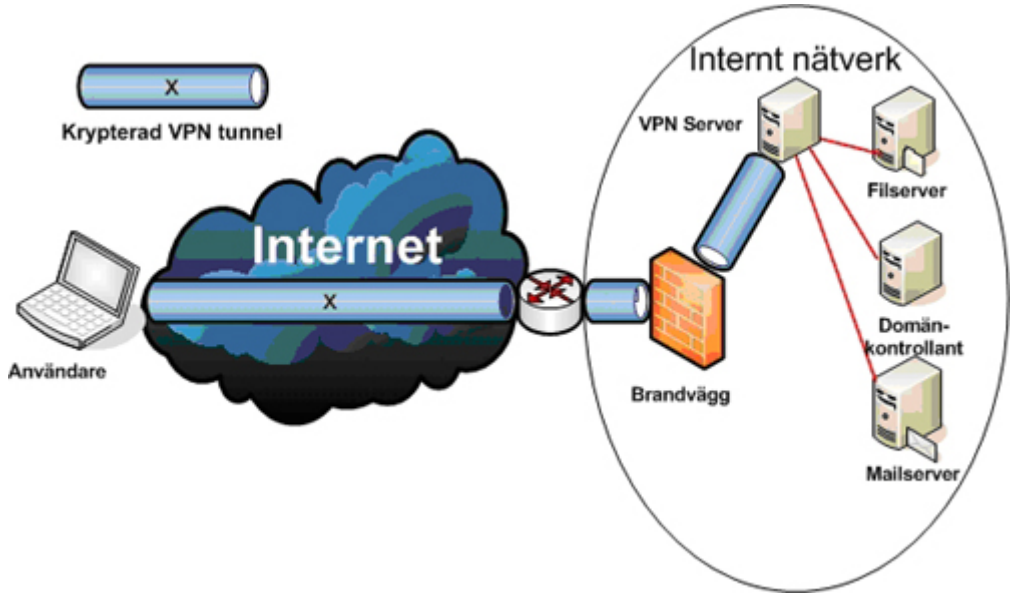
Moderna brandväggar idag klarar av att utföra så kallade tunnelfunktioner. Vilket helt enkelt innebär att brandväggen autentiserar, krypterar och dekrypterar trafiken. Detta innebär att i de fall en användare ansluter hemifrån så kommer trafiken att krypteras mellan användaren och brandväggen. Brandväggen autentiserar användaren och kommer sedan att dekryptera all trafik som kommer från användaren och släppa in den på det lokala nätverket. Brandväggen krypterar dessutom all trafik som går ut från det interna nätverket till samma användare.



Figur 3 Exempel på en brandväggsbaserad VPN lösning.

2.2.3 Serverbaserad VPN-gateway

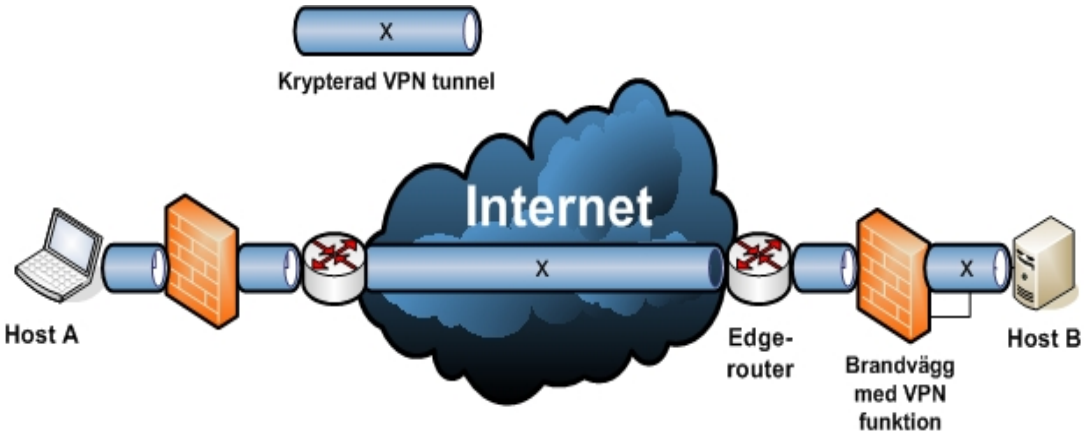
Innebär att man använder sig av en VPN server på insidan av nätverket. Sedan konfigurerar man den befintliga brandväggen så att den skickar krypteringsportarna vidare till den interna VPN-servern. Ett exempel på detta är att installera Windows server 2003 med Routing And Remote Access Service (RRAS). En nackdel med denna metod är att den skapar mer trafik än till exempel brandväggsbaserade lösningar. Vid en anslutning till ett fjärrnätverk går först informationen till vår RRAS tjänst som vanlig trafik, denna kapslas sedan in och krypteras av vår RRAS för att sedan skickas vidare till brandväggen. Detta till skillnad mot brandväggsbaserade VPN-lösningar där paketen kan skickas direkt till brandväggen.



Figur 4 Exempel på en serverbaserad VPN lösning.

2.2.4 VPN-klient

När man kopplar ihop företag med avdelningar på geografiskt skilda platser sker kommunikation mellan ovanstående (router, brandväggs och serverbaserade VPN-gateways) enheter. När däremot en användare vill koppla upp sig mot ett företag måste denna använda sig av en VPN klient som i det flesta fall är en mjukvara som sköter anslutningen mot företagets VPN-gateway.



Figur 5 Exempel på en VPN-lösning där VPN-klient mjukvara används på Host A.

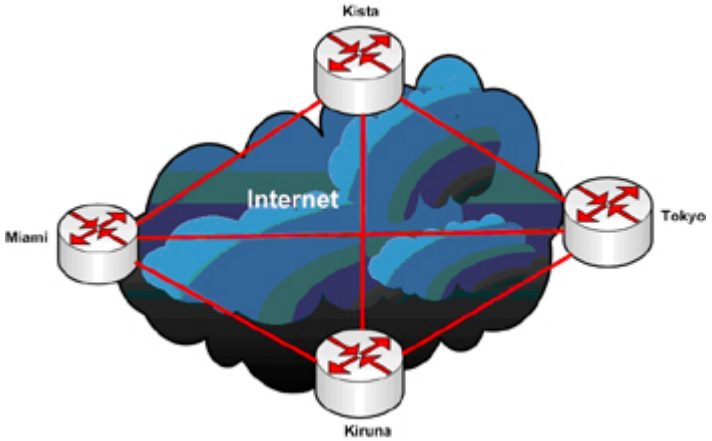
2.3 VPN-Topologier

Det finns olika sätt att bygga upp ett VPN på beroende vad det ska används till och hur mycket redundans som eftersträvas. Nedan beskrivs vanliga topologier där det tre översta vanligen används för att koppla samman företag eller andra organisationer som geografiskt ligger skilda från varandra, medan den sista används för mobila användare.

- Meshed-topologi
- Star-topologi
- Hub and spoke-topologi
- Topologi för mobila användare

2.3.1 Meshed-topologi

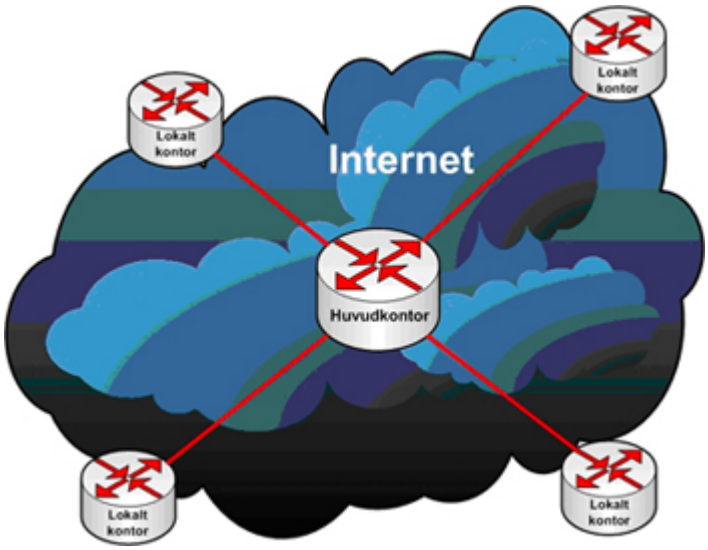
Denna topologi är för de företag som vill ha maximal redundans och åtkomst. Meshed-topologi erbjuder flera vägar till alla destinationer. Detta ger möjlighet att skicka trafiken en annan väg om en av anslutningarna skulle gå ner. Fördelen med denna topologi är att det inte finns någon del i arkitekturen som kan slå ut hela systemet (no single point of failure). Går en VPN-koppling ner kan informationen skickas en annan väg. Nackdelen med topologin är att den kan bli dyr, samt att den är svår att implementera och administrera eftersom man i en stor organisation kommer att behöva massor av tunnlar.



Figur 6 Exempel på ett meshed-topologi nätverk.

2.3.2 Star-Topologi

Denna typ av topologi är vanlig och används ofta av företag som har avdelningar utspridda på geografiskt skilda platser. Topologin bygger på att det finns ett huvudkontor någonstans med information som de lokala avdelningarna behöver. I star-topologin är det inte möjligt för de olika avdelningarna att nå varandra, utan endast huvudkontoret. Denna topologi blir lättadministrerad då bara en tunnel från varje lokal avdelning behöver sättas upp. Ska en ny avdelning upprättas krävs bara två ändringar, en på huvudkontoret samt en på den nya avdelningen. Till skillnad från den ovan beskrivna mesh-topologin där många fler tunnlar måste sättas upp. Största nackdelen med denna lösning är att den inte är lika redundant som mesh-topologin, Skulle huvudkontorets Internetanslutning gå ner skulle inga lokala avdelningar komma åt några resurser.



Figur 7 Exempel på ett star-topologi nätverk.

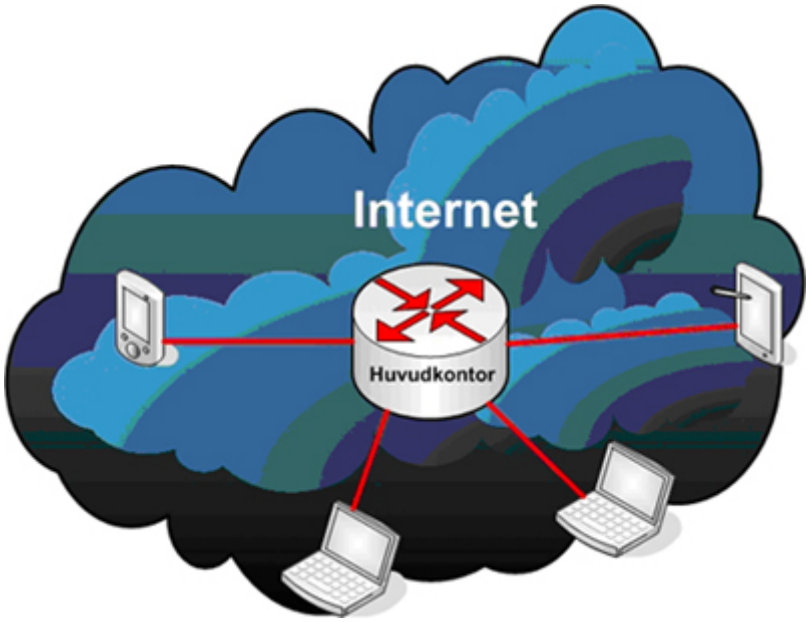
2.3.3 Hub and spoke-topologi

Denna topologi är väldigt lik den tidigare beskrivna star-topologin med den skillnaden att alla avdelningar inte bara kan kontakta huvudkontoret utan även nå varandra via huvudkontoret. Det som sker i denna topologi är att trafiken som kommer till huvudkontoret dekrypteras, inspekteras och skickas vidare till destinationen. Största fördelen är att alla avdelningar kan kommunicera med varandra. Detta bidrar också till en stor nackdel i de fall en hackare får kontroll över en av avdelningarna. Det innebär i så fall att alla avdelningar är i riskzonen eftersom avdelningarna till skillnad från den tidigare beskriva star-topologin tillåts kontakta varandra.

2.3.4 Topologi för mobila användare

De ovan beskrivna teknikerna är alltså mest ämnade för företag som kopplar samman kontor med hjälp av VPN. VPN används i hög utsträckning även för att på ett säkert sätt låta anställda på företag eller i en organisation ansluta till företagets nätverk hemifrån. Metoden som gäller för detta liknar star-topologin ovan där alla användare ansluter genom Internet till en VPN-gateway (se Figur 8 nedan). När det gäller den här typen av VPN-anslutningar så använder sig klienterna av VPN-klientprogram som körs direkt på deras

mobila maskiner. Dom kopplar alltså upp sig med VPN-mjukvaran direkt via Internet till en fast VPN-gateway (till exempel en VPN-gateway på användarens huvudkontor)



Figur 8 Exempel på mobila användare med inbyggda VPN-klientprogram som ansluter till ett företags VPN-gateway.

2.4 VPN-Protokoll

Det finns ett antal olika protokoll för att skapa "säkra" tunnlar mellan två ändpunkter. Man bör noga undersöka olika alternativ innan man implementerar en VPN lösning. Eftersom vi i vårt examensarbete hade tre valmöjligheter PPTP, L2TP/IPSec och IPSec så har vi studerat och beskrivet dessa nedan. En vanlig lösning som är på frammarsch som också bör nämnas är SSL VPN.

2.4.1 Point-to-Point Tunneling Protocol (PPTP)

Detta är ett protokoll som arbetar i det andra skiktet i Open Systems Interconnection OSI modellen, det så kallade datalänkskiktet. PPTP utvecklades av Microsoft och 3COM och fanns tillgängligt redan i Microsoft NT

PPTP är en utbyggnad av Point to Point Protocol (PPP) protokollet kapslar in PPP-paket i ett Internet Protocol (IP) paket. Anledningen till att detta görs är för att IP kan routas på Internet. För att kunna förklara detta lite noggrannare bör vi veta vad PPP-protkollet gör.

PPP är ett nätverksprotokoll som används för att hantera fjärranslutningar från klienter till servrar via en uppringd förbindelse. En vanlig användning av PPP är när man som klient upprättar en anslutning till Internet eller sin Internet Service Provider (ISP) via modem. PPP-protokollet kapslar in ett IP-paket i PPP-ramar vilket påminner om inkapslingen av IP i Ethernet ramar. Dessa paket kan sedan användas för att skapa en punkt-till-punkt förbindelse mellan den sändande och den mottagande datorn. För noggrannare genomgång av PPP-protokollet läs avsnitt 2.5

När en klient ansluter till en PPTP-server så sker följande. Klienten har ett IP-paket som denne vill sända till ett privat nät. Detta IP-paket kapslas in i en PPP-ram för att åstadkomma en punkt-till-punkt förbindelse till PPTP-servern. För att denna PPP-ram skall

kunna routas till rätt adress på Internet så kapslar PPTP mjukvaran in även detta paket i ett IP paket. Så här kommer således ett paket som lämnar klienten att se ut (Figur 9).

IP	GRE	PPP	IP	TCP	DATA

Figur 9 Där TCP står för Transmission Control Protocol

Generic Routing Protocol (GRE) i IP-paketet är det så kallade tunnelprotokoll som packar in PPP-paketet i ett IP-paket. Det är PPP-protokollet som står för användarautentiseringen, autentiseringsmetoder som kan användas är Password Authentication Protocol (PAP), CHAP (Challenge Handshake Authentication Protocol) och eller EAP-TLS (EAP Transport Layer Security, där EAP står för Extensible Authentication Protocol). Krypteringen i PPTP trafik sköts av Microsofts Point-to-Point Encryption (MPPE). Krypteringsalgoritmen som används är RC4 och tillåter 40, 56 och 128 bitars nycklar. För att tillåta denna kommunikation så måste TCP port 1723 var öppen i eventuella brandväggar.

Källor: [1], [2], [3].

2.4.2 IP Security

IP Security (IPSec) är ett standardprotokoll som fungerar med IP-protokollet. IPSec befinner sig i nätverksskiktet av OSI-modellen. IPSec har utvecklats av Internet Enginering Task Force (IETF) för att öka säkerheten vid IP kommunikation. IPSec kan användas i en punkt till punkt förbindelse mellan två datorer för att göra kommunikationen säker. IPSec kan också användas i VPN för att ge en säker kommunikation mellan en anslutande klient och en VPN-server. IPSec är inte ett protokoll utan snarare en protokollstack som tar hjälp av flera protokoll för att utföra sina mål konfidentialitet, integritet och autentisering. För att lättare förstå kan man dela in IPSec i två delar.

- **Security Protocols**. Är de protokoll som definierar vilken information som ska läggas till ett vanligt IP-paket för att uppnå just konfidentialitet, integritet och autentisering.

- **Internet Key Exchange** (IKE). Genom IKE autentiseras två enheter mot varandra, utväxlar en hemlig sessionsnyckel för att kryptera och dekryptera data samt enas om vilka protokoll som skall användas.

2.4.2.1 Security Protocols

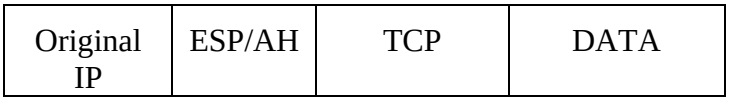
Innan vi går djupare in på dessa säkerhetsprotokoll i IPSec så bör vi först förstå de två olika lägen som IPSec kan köras i, nämligen tunnel mode och transport mode. För att förstå skillnaderna mellan dessa bör vi först veta hur ett vanligt IP-paket ser ut (se Figur 10 nedan).

Original IP	TCP	DATA

Figur 10 Enkelt ritat IP-paket.

I transport mode ändras bara datalasten i ett paket vilket innebär att IP-huvudet är intakt. Detta läge används när mottagaren och sändaren är ändpunkter i kommunikationen. Till

exempel när två datorer pratar direkt med varandra och bara den ena av dessa känner till den andres adress. Nedan illustreras hur ett IPSec-paket ser ut i Transport mode. Fältet ESP/AH beskrivs längre ner i detta avsnitt.



Figur 11 IPSec-paket i transport mode

I tunnel läget däremot kapslas hela det ursprungliga paketet istället in i ett nytt paket och ett nytt IP huvud skapas. Tunnel-läget används i site-to-site lösningar där två VPN-gateways pratar direkt med varandra, dessa har oftast fasta IP-adresser. Nedan i Figur 12 visas hur ett IPSec-paket kommer att se ut i tunnel mode

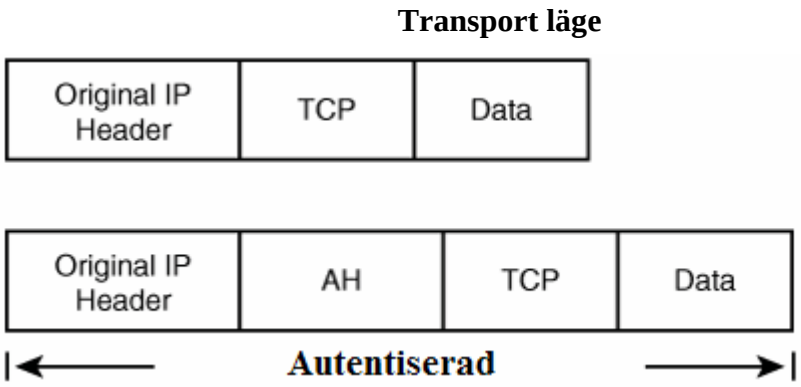
Figur 12 IPSec-paket i tunnel mode

Huvudsyftet med IPSec är som sagt att ge säkerhet till vanliga IP-paket. Tjänster som IPSec använder/tillhandahåller för att göra kommunikationen säkrare är bland annat dataintegritet, autentisering, skydd mot återspelningsattacker och datakryptering. För att kunna ge dessa skydd till IP-paket använder sig IPSec av två protokoll: Encapsulating Security Payload (ESP) och Authentication Header (AH).

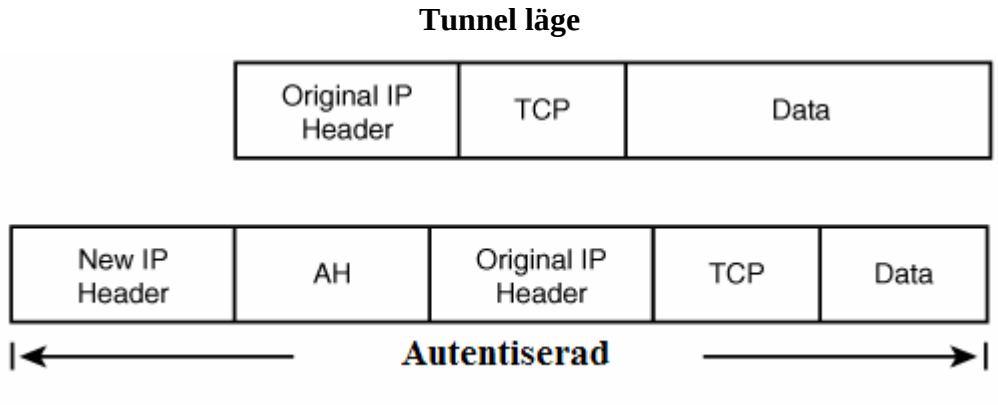
2.4.2.1.1 Authentication Header (AH)

Detta IPSec-protokoll gör en digital signering av IP-huvudet i varje paket som ingår i IPSec överföringen. Mottagande dator verifierar signaturen i varje paket genom att använda sig av en sessionsnyckel som delas mellan parterna. Om någon bit av paketet har förändrats under transporten kommer mottagande dator att slänga paketet. Genom att göra detta kan man vara säker på att IP-paketet inte förändrats under transporten. Man kan också vara säker på att den som skickat paketet är en legitim användare eftersom bara en sådan kan signera ett IP-paket med en giltig sessionsnyckel. Notera att AH inte krypterar datalasten. Genom att beräkna ett hashvärde av hela IP-paketet och skicka med det till mottagaren kan integritet uppnås. Detta kallas Integrity Check Value (ICV). Sändaren beräknar ett hashvärde av paketet med hjälp av en hashfunktion eller Message Authentication Code (MAC) som det också kallas. För att skapa integritet så använder sändaren också ett värde i hashfunktionen som bara är känt mellan de kommunicerande parterna. När mottagaren sedan tar emot paketet beräknas hashvärdet på samma sätt av mottagaren. Om ICV-fältet stämmer med mottagarens beräkningar anses paketet vara giltigt och tas emot. Hashfunktioner som används av IPSec för detta ändamål är vanligen Message-Digest algorithm 5 (MD5) och Secure Hash Algorithm 1 (SHA1). Det bör nämnas att på senare tid har lyckade attacker mot dessa protokoll gjorts och en ny standard håller på att tas fram. Den säkrare av dem är SHA-1. AH ger också skydd mot uppspelning av trafik via en enkel räknare i AH-huvudet. Denna räknare ger varje paket ett sekvensnummer och slänger paket som kommer i fel ordning.

Nedan visas hur ett paket påverkas när man använder AH i transport-(Figur 13) respektive tunnel-(Figur 14) läge.



Figur 13 Visar hur AH används i Transport läge i ett IPSec paket

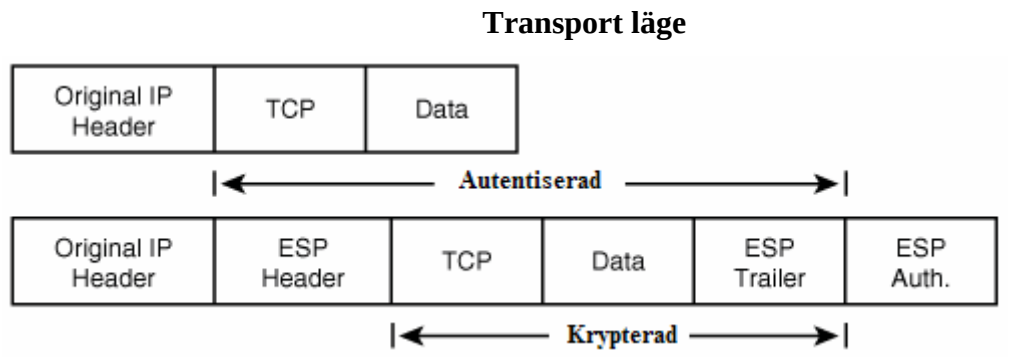


Figur 14 Visar hur AH används i Tunnel läge i ett IPSec paket

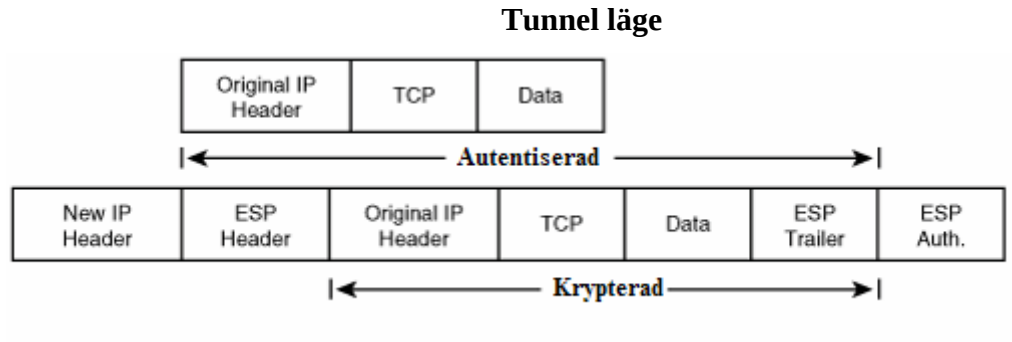
2.4.2.1.2 Encapsulating Security Payload (ESP)

ESP har samma funktioner som AH men ser även till att kryptera datalasten. ESP krypterar och autentiserar hela paketinnehållet genom att använda sig av en delad sessionsnyckel. Mottagande dator använder sig av samma sessionsnyckel för att dekryptera paketet. Skillnaden mellan AH och ESP är alltså att ESP kan kryptera datalasten. Krypteringen skiljer sig en del beroende på om man använder tunnel- eller transport-läget. I tunnel-läget krypteras original IP-adressen medan det nya IP-huvudet lämnas orörd. I transport-läget lämnas original IP-adressen däremot orörd medan resten av paketet krypteras. Autentiseringen skiljer en del från AH. Skillnaden där är att i ESP är hash-summan inte beräknad på hela paketet utan bara på den del som har med ESP att göra. ESP tar inte med det yttersta IP-huvudet i beräkningen av hash-summan. I ESP används samma hashfunktioner som i AH. De krypteringsalgoritmer som används är oftast Data Encryption Standard (DES), Triple DES (TDES).

Nedan visas hur ett paket påverkas när man använder ESP i transport (Figur 15) respektive tunnel (Figur 16) läge.



Figur 15 Visar hur ESP används i Transport läge i ett IPSec paket



Figur 16 Visar hur ESP används i Tunnel läge i ett IPSec paket

Källa: [4]

2.4.2.2 Internet Key Exchange (IKE)

IKE är egentligen inte ett protokoll utan en samling protokoll, bland annat ingår Internet Security Association and Key Management (ISAKMP) och Oakley key determination protocol. Dessa protokoll används för att skapa en säker kanal mellan två kommunicerande parter.

För att kunna kommunicera säkert mellan två parter använder sig IPSec bland annat av kryptering och autentisering. För att vi skall kunna använda oss av kryptering och autentisering gäller det att parterna är överens om vilka metoder som skall användas för detta. Innan kommunikationen kan börja på ett säkert sätt måste man också utbyta en hemlig sessionsnyckel mellan parterna samt autentisera parterna för varandra. Eftersom sessionsnycklen är hemlig och man vill att den ska förbli så, byter man denna med jämna mellanrum. Hur ofta detta ska ske bestäms också det i uppstarten av kommunikationen. Alla de parametrar som förhandlas fram mellan de två parterna av IKE sparas i en Security Association (SA) som i sin tur sparas på varje dator i en SA Database (SAD). Varje paket som skickas mellan två enheter som kommunicerar med IPSec kommer att ha ett värde kallat Security Parameter Index (SPI). När ett paket anländer till en enhet kollar den på SPI-värdet och med hjälp av detta kan den kolla i SAD och se vilken SA den skall använda sig av i kommunikationen. Det finns två typer av SA:

- IKE SA
- IPSec SA

2.4.2.2.1 IKE SA

Första delen sköter autentisering, byte av sessionsnyckel och enas om användningen av protokoll. Resultatet av denna förhandling blir en IKE SA. För att sköta detta första utbyte säkert använder sig IKE av ISAKMP protokollet.

IKE arbetar i två faser. Fas 1 börjar när två kommunicerande parter behöver upprätta en säker anslutning. Vid det här laget finns alltså ingen SA etablerad. IKE fas 1 kan ske i två lägen nämligen main mode och aggressive mode. Main mode är säkrare men något långsammare än aggressive mode. Main mode sker i tre steg. Detta innebär att sex meddelanden kommer att skickas mellan parterna då varje steg sker i båda riktningarna. Nedan beskrivs de tre stegen i main mode.

- **Steg 1:** Det första som sker är att parterna kommer överens om vilka algoritmer som skall användas för att säkra kommunikationen. T.ex. 3DES och SHA1.

- **Steg 2:** I det här steget används Diffie Hellman protokollet för att skapa en hemlig nyckel mellan parterna.(Se kapitel 2.7.1.1 för mer information om DH)

- **Steg 3:** I sista steget i fas 1 autentiseras parterna för varandra. IKE protokollet tillåter flera olika autentiseringsmetoder (Mer information om dessa metoder i kapitel 2.4.3). Värt att notera är att denna information kommer att skyddas med hjälp av den sessionsnyckel som skapades i steg 2. Detta innebär att autentiseringsinformationen som skickas här kommer att vara krypterad.

Skillnaden mellan main mode och aggressive mode är att den senare klarar detta utbyte med bara 3 meddelanden. Informationen om algoritmer och skapandet av sessionsnycklar via Diffie Hellman skickas i samma meddelande. Mottagaren skickar tillbaka allting som behövs för att slutföra det första steget. Allt detta sker alltså med bara 2 meddelanden. Ett tredje och sista meddelande skickas av sändaren för att bekräfta utbytet. Svagheten med Aggressive mode är att båda sidor utbyter information innan en säker kanal har skapats. Det är därför möjligt att läsa av viss information i utbytet Fördelen med aggressive mode är att det är snabbare än main mode. Båda dessa metoder kan användas för att skapa en IKE SA. När denna är etablerad så tar fas 2 vid.

Källa: [5], [6].

2.4.2.2.2 IPSec SA

Dessa skapas i fas 2. IPSec SA är det som används för att säkra kommunikationen av data. Man använder sig av en metod kallad Quick Mode i fas 2 och följande funktioner uppnås.

- Förhandlar om IPSec SA parametrar. Denna förhandling är skyddad av den IKE SA som skapades i fas 1.

- Skapar IPSec SA

- Förhandlar vid ett givet tidsintervall eller när en viss mängd data passerat fram en ny IPSec SA för att bibehålla säkerheten i kommunikationen.

- Kan göra ett nytt Diffie Hellman utbyte. Detta är valfritt, men stärker också säkerheten något då sessionsnycklar förnyas. Detta kallas även Perfect Forward Secrecy (PFS).

När Quick mode är avslutat är IPSec tunneln upprättad. Trafiken mellan parterna kommer nu att skyddas av de krypterings- och autentiseringsmetoder som förhandlats fram under Quick mode. En IPSec SA tas bort genom att man kopplar ner anslutning eller genom att livstiden går ut. Man kan ställa in en IPSec SAs livstid antingen genom att sätta ett visst antal sekunder eller när en viss datamängd har passerat genom tunneln. Om IPSec SA fortfarande används då livstiden håller på att gå ut så kan IPSec göra ett nytt fas 2 utbyte och på så sätt kan kommunikationen fortgå.

2.4.3 Autentisering i IPSec

2.4.3.1 Pre-Shared key

Med pre-shared key är samma nyckel manuellt inställd på båda parterna som deltar i kommunikationen. Ett hashvärde beräknas med information från nyckeln och skickas till motparten i kommunikationen. Motparten utför samma beräkning med sin nyckel och jämför det värdet med värdet som den fick av motparten. Stämmer värdet vet de att de delar nyckel och kommunikationen kan fortsätta. Nackdelen med denna metod är att alla användare som ansluter använder samma pre-shared key. Givetvis kan någon antingen av illvilja eller av misstag avslöja nyckeln. Den bästa metoden är att inte ge användarna nyckeln genom att som administratör skriva i den åt användaren eller på annat sätt distribuera den. Skulle någon knäcka nyckeln så skulle alla datorer på företaget samt VPN gatewayen få konfigureras om vilket kan vara ett stort jobb i en stor organisation. Därför lämpas den lösning bäst för mindre företag. För att göra det svårt att knäcka eller gissa nyckeln ska den göras komplex. Nyckeln bör vara minst 8 tecken och varieras med gemener, versaler, siffror och specialtecken.

2.4.3.2 Certifikat

Detta är den säkraste och mest skalbara lösningen att sköta autentiseringen i IPSec på. Med denna metod slipper man lösenordshanteringen som finns i pre-shared key varianten. Istället blir användare och tjänster tilldelade ett certifikat av en så kallad Certficate Authority (CA), som fungerar som en betrodd tredje part. Ett certifikat innehåller bland annat ett namn och en publik nyckel samt en tidpunkt då certifikatet upphör att gälla. En CA skapar certifikatet och signerar det med sin privata nyckel, För att kunna kontrollera signeringen krävs tillgång till samma CA:s publika nyckel, som bara legitima användare har tillgång till. Mer information om certifikat som autentisering finns i kapitel 2.8

2.4.3.3 Kerberos

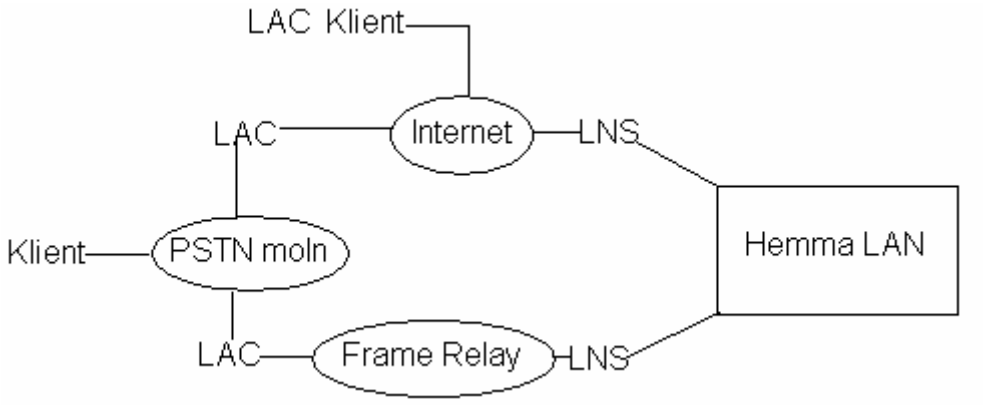
Kerberos är ett är ett protokoll som förlitar sig på en servertjänst eller Key Distribution Center (KDC) som det också kallas. Kort går det ut på att en användare identifierar sig hos servern med namn och lösenord och om dessa är korrekta tilldelas användaren en Ticket Granting Ticket (TGT). Denna kan i sin tur användas för att exempelvis autentisera sig för en tjänst. Normalt används denna typ av autentisering på privata nät, och är därför lämplig att implementera när man använder sig av IPSec på ett privat nät.

Övriga källor IPSec: [7], [8], [9], [10].

2.4.4 Layer 2 Tunneling Protocol (L2TP)

PPP är det protokoll som används till att kapsla in nätverkslagerprotokoll och skicka dessa över lager 2 punkt-till-punkt länkar. Vanligtvis får en användare en lager 2 anslutning till en L2TP Access Concentrator (LAC, som tillhandahålls av ISP'n) genom en av många tekniker (till exempel modemanslutning via telefonnätet, ISDN eller ADSL) och använder sedan PPP-protokollet över dessa medium. I de här fallen kommer lager 2 anslutningen och PPP-protokollets ändpunkt vara den samma, det vill säga i LAC:en.

Det L2TP gör är att tillåta olika ändpunkter för PPP och lager 2 anslutningar. Med L2TP skapas en lager 2 anslutning till en ISP:s anslutningspunkt (LAC), till denna enhet är det PPP-protokollet som används. Anslutningspunkten skickar sedan vidare PPP-paketen till en L2TP Network Server (LNS, kan vara ett företags VPN-gateway) som ligger på andra sidan ett paket förmedlande nätverk såsom Internet eller Frame Relay. Det man tjänar in på den här lösningen är att man kan ringa upp en lokal lager 2 anslutningspunkt som sedan skickar paketen vidare över ett billigare medium (till exempel Internet) till mottagarens LNS-enhet, istället för att klienten måste göra en punkt till punkt anslutning direkt till mottagarens enhet som kanske står på andra sidan jordklotet. På så sätt blir det betydligt billigare.

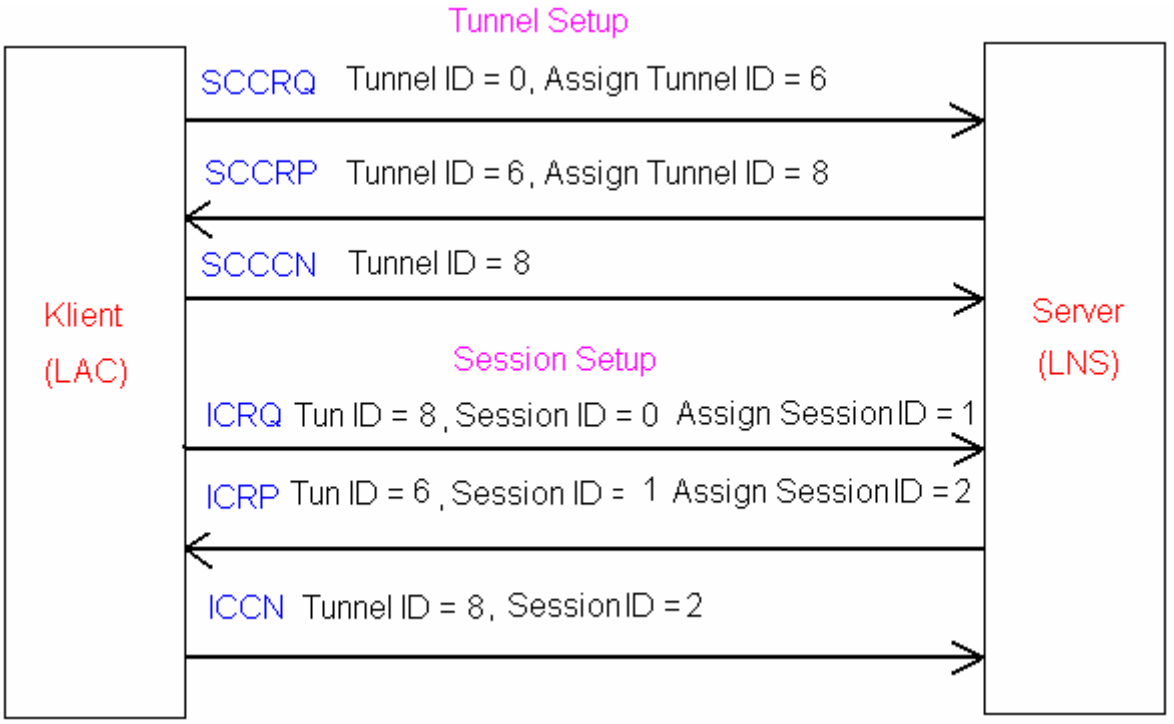


Figur 17 Olika exempel på hur L2TP kan användas.

Figur 17 ovan visar hur olika L2TP-tunnlar kan se ut. Anslutningen börjar hos klienten som ringer upp sin anslutningspunkt som vi kallar för L2TP Access Concentrator (LAC) det kan vara en Modem bank eller ADSL DSLAM. LAC tunnlar sedan PPP paketen vidare över Internet eller Frame Relay till en L2TP Network Server (LNS) som kan vara en brandvägg eller en server som klarar av L2TP. LNS ger åtkomst till nätverket och via PPP-förhandling kan användaren få en lokal IP-adress. Autentisering, behörighet och konto kontroll kan utföras på det lokala nätverket genom till exempel RADIUS. Ett annat sätt att upprätta en L2TP-anslutning är att klienten agerar som LAC genom att använda någon form av L2TP-mjukvara. På så sätt kan en klient uppkopplad direkt mot Internet använda sig av L2TP's funktioner.

L2TP använder sig av två olika meddelande typer control- eller datapaket. Lättast att förstå hur dessa används är att beskriva hur en L2TP-anslutning upprättas och används när den väl är uppe. Det börjar med att LAC-enheten antingen en LAC-klientprogramvara eller en LAC-enhet hos en ISP skickar ett Start-Control-Connection-Request (SCCRQ) paket till LNS. Det här meddelandet innehåller: Host name, protokoll version, tunnel ID, inramnings möjligheter och meddelande typ Attribute Value Pair (AVP, en form av ID värde) utöver dessa informationsfält finns det ytterliggare 6 som är frivilliga. På det här meddelandet svarar LNS med ett Start-Control-Connection-Reply (SCCRP) meddelande som indikerar

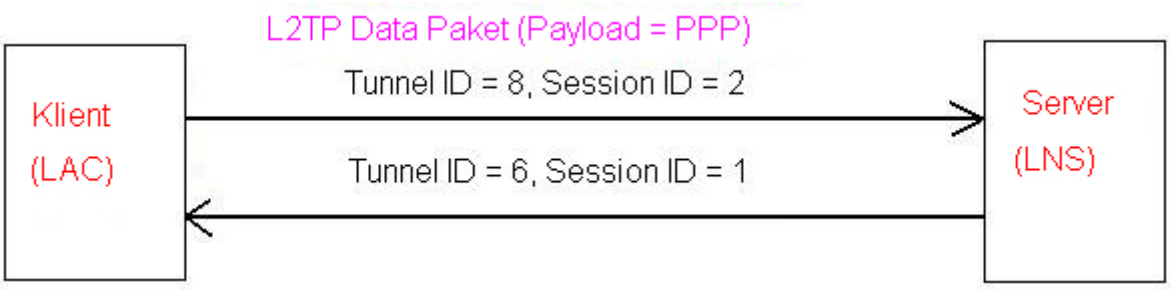
att LNS har godkänt de parametrar som skickades med i SCCRQ meddelandet. När dessa två meddelanden har skickats svarar LAC med ett Start-Control-Connection-Connected (SCCCN) meddelande, när detta har mottagits är själva L2TP-tunneln uppe. För att högre-lager-protokoll (till exempel PPP) skall kunna använda tunneln krävs det att en session per protokoll upprättas inne i tunneln. Detta sker på samma sätt som ovan, med ett tre-stegs-meddelande-utbyte som börjar med att LAC skickar ett Incoming-Call-Reguest (ICRQ) meddelande till LNS, eller tvärtom att LNS skickar ett Outgoing-Call-Request (OCRQ) till LAC. En session kan alltså upprättas från både en LAC eller en LNS. Skillnaden mellan dessa är att när LNS gör uppringningen så måste paketet innehålla fler parametrar än om anslutningen upprättas från LAC. Det andra steget i upprättandet av en session är när Incoming-Call-Reply (ICRP) och motsvarande Outgoing-Call-Reply (OCRP) paket skickas som svar på förfrågningarna. Båda dessa innehåller samma data: Meddelande typ och tilldelat sessions ID. Efter dessa meddelanden följer ett Incoming-Call-Connected (ICCN) eller motsvarande Outgoing-Call-Connected (OCCN) paket som talar om att alla parametrar har blivit godkända och att sessionsanslutningen nu är upprättad. I de här meddelanden är det bara tre obligatoriska fält: meddelande typ, anslutnings hastighet och inramnings typ.



Figur 18 Anslutningsfas i L2TP.[11]

Dessa meddelanden är alla av typen control-meddelanden som skickas över en separat kanal i tunneln och används till att sätta upp och underhålla tunneln och de olika sessionerna. För varje L2TP-tunnel finns det en control-kanal och en eller flera sessioner. Mellan en LAC och LNS kan man sätta upp en eller flera L2TP-tunnlar. En stor skillnad mellan control- och data-meddelanden är att control-meddelanden återskickas om ett meddelande inte skulle komma fram. Både LAC och LNS måste ha en sekvensnummer tabell där de håller reda på vilka control paket de fått och på så sätt kan se om något paket inte kommit fram och då begära en omsändning av det förlorade paketet. Data-meddelanden har dock inte den här funktionen och därför sker inga omsändningar av förlorade paket. Som sagt så används control-meddelanden till att upprätta tunneln och de

olika sessionerna i den. När dessa är upprättade med en sessions kanal för PPP så används Data meddelanden för att skicka själva PPP-ramarna (Se Figur 19 nedan).



Figur 19 Visar hur ID fälten används under datapaket sändning [11].

En L2TP-ram ser olika ut beroende på om det är en control- eller data-ram. Nedan i Figur 20 visas alla fält som kan ingå i ett L2TP-ram huvud.

2 Bytes	2 Bytes
Flags & Version info	Length (opt.)
Tunnel ID	Session ID
Ns (opt)	Nr (opt)
Offset Size (opt)	Offset pad.. (opt)

Figur 20 L2TP ramhuvud

Bitar

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8

|T|L|x|x|S|x|O|P|x|x|x|x| Version

Figur 21 Visar dom olika flaggorna i Flags & Version fältet.

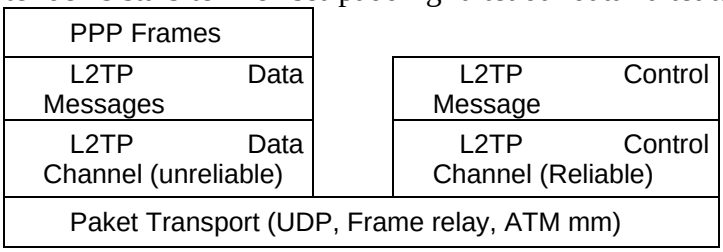
I det första fältet Flags & version indikerar de 12 första bitarna olika saker se figur Figur 21. Den första biten T sätts till 0 om det är ett data paket och till 1 om det är ett control-paket. L biten som är den andra berättar om Length fältet används, när paketet är ett control-paket måste denna bit sättas till 1 vilket betyder att det används. Alla bitar med x är reserverade för framtida bruk och måste vara satta till 0. S biten talar om hur vida Ns och Nr fälten används, dessa fält är sekvensfälten och måste användas i control-paketen. En 1 indikerar att de används. Efter den biten kommer offset (O) biten som indikerar om offset-size fältet används, en 1 betyder att det används. O biten måste vara satt till 0 när det är ett control-paket. Priority (P) biten används bara av data-paket, satt till 1 betyder att data-paketet går före i sändnings kön. Detta används när data-paketet innehåller till exempel ett LCP Keep-alive-paket, om detta måste vänta på sin tur i kön kan den extra tiden innebära att länken kopplas ner. Vid ett control-paket är detta värde alltid satt till 0. Version (Ver) indikerar att detta är ett L2TP-paket då det är satt till 2. Om det är satt till 1 indikerar det istället att paketet är av typen Layer 2 Forwarding (L2F ett äldre Cisco VPN protokoll) protokoll.

Det andra fältet Length, talar om hur stort meddelandet är totalt.

Tunnel ID fältet innehåller ID numret för tunneln. de båda ändarna har var sitt Tunnel ID för samma tunnel (Se Figur 18). Session ID fältet fungerar på samma sätt fast indikerar istället ID för en specifik Session. ID som står i dessa två protokoll är ID som mottagaren av paketet har och inte det sändaren har.

De nästkommande två fälten Ns och Nr indikerar sekvensnummer. Ns sekvensnumret för just det här paketet och Nr det förväntade sekvensnumret för nästa paket.

Offset-size fältet talar om hur många bitar efter L2TP-huvudet som själva data-fältet börjar. Själva offset-padding fältet är odefinierat. Om offset-size fältet används så slutar L2TP-ram huvudet direkt efter den sista biten i offset-padding fältet där data-fältet tar vid.



Figur 22 Visar hur Data och Control paketen används.

När man skickar ett PPP-paket kapslas detta in i en L2TP-dataram (PPP-paketet ligger i data-fältet) som sedan kapslas in i själva bärarprotokollet (se Figur 22 ovan). Vilket bärarprotokoll som används beror på vilket medium kommunikationen går över. Över Internet används UDP som bärarprotokoll. När L2TP skickas med UDP så packas hela L2TP paketet in i en UDP-ram. L2TP-paketet läggs i UDP-paketets data-fält, sedan skickas UDP-paketet till mottagarens adress på port 1701.

Källa: [12].

2.4.4.1 L2TP över IPSec

Eftersom L2TP skickar sina paket enbart inkapslade i ett UDP-paket direkt över IP-nätverk så är det väldigt lätt att snappa åt sig dessa paket längs vägen och läsa innehållet i klartext. Några av säkerhetsriskerna med detta kan vara:

- Någon kan försöka ta reda på användardata såsom lösenord och användarnamn genom att undersöka paket som snappats upp
- Paketdata kan ändras på vägen.
- Någon kan kapa L2TP-tunneln eller PPP-anslutningen inuti tunneln.
- Någon kan utföra denial-of-service attacker genom att avsluta PPP-sessioner eller L2TP-tunneln. På så sätt blir VPN-tjänsten oanvändbar då det för användaren kommer se ut som den kopplar ifrån hela tiden.

För att motverka dessa hot måste L2TP använda sig av ett säkerhetsprotokoll som klarar av att stå emot dessa attacker. Det ä nu IPSec kommer in i bilden, IPSec tillhandahåller detta genom kryptering av paket och maskin autentisering (läs mer om IPSec i avsnitt 2.4.2). Ett UDP-paket innehållandes ett L2TP-paket bakas in i ett IPSec-paket på följande vis(Se Figur 23 nedan), där de kursiva fälten är de fält som är krypterade.

IP header	IPSec ESP header	*UDP header*	*L2TP header*	*PPP header*	*PPP Payload*	*IPSec ESP trailer*	IPSec Auth trailer

Figur 23 L2TP paket inbakat i IPSec [13].

Källa: [14].

2.5 Point to point protocol (PPP)

PPP kom till som ett transportprotokoll för IP-trafik över punkt-till-punkt länkar. Den kan hantera både synkron och asynkron kommunikation och upptäcker fel. Uppgifter som PPP designades för att klara av är tilldelning och hantering av IP adresser, klara av fler protokoll än bara IP, länk konfiguration, länk kvalitets kontroll och förhandling av datakompression. PPP klarar av dessa saker genom att använda sig av en Link Control Protocol (LCP) för att upprätta punkt till punkt länken och ett Network Control protocol (NCP) för att konfigurera de olika nätverkslagerprotokollen som kan användas tillsammans med PPP. En annan viktig funktion PPP använder sig av är autentisering vid upprättande av en anslutning och periodvis under en pågående anslutning. De autentiseringsprotokoll PPP kan använda sig av är PAP eller CHAP.

1 Byte	1 Byte	1 Byte	2 Byte	Variable	2 or 4 Byte
Flag	Address	Control	Protocol	Data	FCS

Information	Padding

Tabell 1 PPP paket i HDLC format

Ett PPP-paket består utav 6 olika fält.

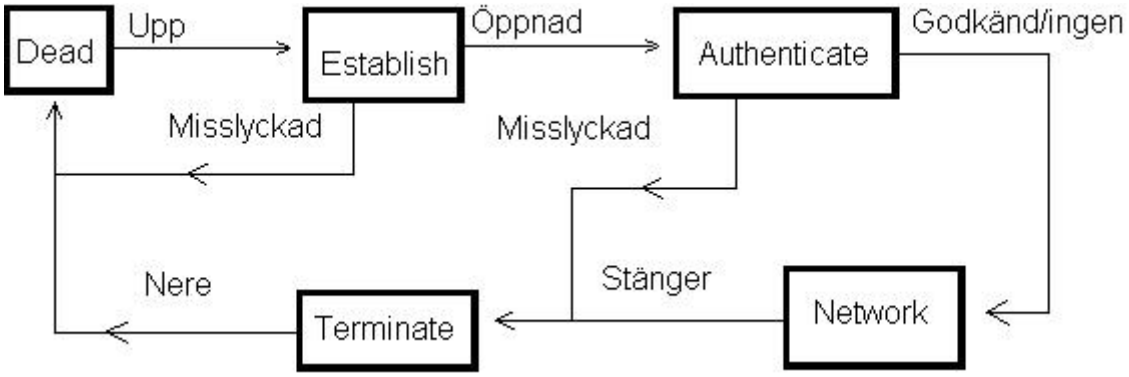
Först kommer Flag fältet som indikerar början på ett nytt paket och slutet på paketet innan och innehåller den binära sekvensen 01111110. Det räcker alltså med ett Flag fält mellan två paket.

Efter det är det Address fältet på 1 Byte som innehåller broadcast adressen 11111111. PPP tilldelar inte individuella adresser.

Control fältet innehåller den binära koden 00000011 och talar om att det kommer användardata i ett onumrerat paket.

Efter dessa 3 fält kommer vi fram till det egentliga PPP-paketet som består av 3 fält. Protocol-fältet som talar om vilket nätverkslagerprotokoll som ligger inkapslat i data fältet. Data-fältet består av 2 Fält. Först Information-fältet som innehåller data från nätverkslagerprotokollet. Efter det kommer Padding fältet som kan innehålla utfyllnadsbitar för att komma upp i rätt paketstorlek (Maximum Receive Unit = MRU).

Upprättandet av en anslutning över en punkt till punkt länk går till så att PPP först skickar LCP paket för att konfigurera och testa datalänken. Efter att LCP har fått upp länken sker autentiseringen om den är vald. När detta är klart och länken är uppe så skickas NCP paket iväg för att förhandla om vilka nätverkslagerprotokoll som skall användas. Så fort detta är klart kan paket från de olika nätverkslagerprotokollen börja skickas över länken. Själva länken kommer vara uppe så länge ett LCP eller NCP paket inte skickas för att stänga ner den, en viss tids inaktivitet så att en timer går ut eller en användare lägger sig i. Punkt till punkt länkens olika faser kan lättast beskrivas med ett flödesschema (se Figur 24 nedan)



Figur 24 Visar de olika anslutningsfaserna i en PPP anslutning.

Innan en anslutning börjar ligger de båda parterna i Dead (väntande) läge. När en nätverksadministratör konfigurerar en anslutning eller en bärare detekteras (ett modem kanske sätts på) går man vidare till Link Establishment-fasen och Upp signaleras. När Upp har signalerats tar LCP vid för att förhandla fram parametrarna som ska användas vid kommunikationen. Om en parameter inte står med antas ett default-värde för den parametern. De parametrar som finns är följande: 1 MRU, 3 Authentication-protocol, 4 Quality-Protocol, 5 Magic-Number, 7 Protocol-Field-Compression, 8 Address-and-Control-Field-Compression. Den här fasen är klar när båda parterna har skickat ett Configure-Ack paket.

Nu går LCP in i Öppnad läget. Om autentisering förhandlades fram i parameter förhandlingen så är det nu den sker, autentisering sker bara om den förhandlas fram. Som standard är det ingen autentisering och Network fasen tar vid. Om autentisering är vald så sker den med antingen PAP eller CHAP. När anslutningen väl har kommit till Network fasen så är det dags för de nätverkslagerprotokoll som skall användas att förhandla fram parametrar via deras egna NCP-protokoll. Några exempel på nätverkslagerprotokoll och dess NCP-protkoll är IP som använder IP Control Protocol (IPCP), Internetwork Packet Exchange (IPX) som använder Novell IPX Control Protocol (IPXCP) eller AppleTalk. I den här fasen kan en blandning av LCP, NCP och nätverkslagerprotokoll skickas över länken. När som helst under en aktiv länksession kan länken stängas ner, detta kan bero på flera olika saker så som en misslyckad autentisering, länkkvaliteten är för låg, en timer går ut eller helt enkelt så att modemet stängs av. Det är LCP som sköter om avstängningen genom utbyten av Terminate-paket.

Det finns tre typer av LCP-paket:

1. LCP paket som används till att konfigurera en länk, dessa paket är Configure-Request, Configure-Ack, Configure-Nak och Configure-Reject

2. Paket till för att avsluta en länk, Terminate-Request, Terminate-Ack

3. Paket för underhåll och felsökning av länken såsom Code-Reject, Echo-Request, Echo-Reply och Discard-Request.

Själva LCP paketet ser ut som nedan (Tabell 2, LCP paket)

1 Byte	1 Byte	2 Byte
Code	Identifier	Length
Data …		

Tabell 2, LCP paket

Code fältet talar om vilken typ av LCP-paket som skickas (se i texten ovanför Tabell 2, LCP paket). Identifier (ID) fältet fungerar som dom flesta andra ID fält gör, används alltså till att matcha svar mot förfrågningar. Length-fältet likaså, det talar om den totala storleken på LCP-paketet. Storleken här får inte överskrida MRU. Data fältets utseende bestäms av vilket LCP-paket som skickas.

LCP paketet ligger i PPP-paketets information fält och exakt ett LCP-paket skickas med ett PPP-paket. LCP har den hexadecimala koden c021 i PPP-paketets Protocol fält.

Källor: [15], [16], [17].

2.6 Challenge handshake password (CHAP)

CHAP protokollet används till att verifiera identiteten hos en klient. Detta sker när en PPP-anslutning upprättas med hjälp av 3 meddelanden, så kallad 3-way handshake, men kan även ske när som helst medan anslutningen är igång. CHAP-autentiseringen går till på följande vis:

1. När PPP-anslutningen är uppe skickar klientens motpart ett ”Challenge” meddelande till klienten.

2. Klienten svarar på ”Challenge” meddelandet med ett värde som räknats fram med en envägs hashfunktion.

3. Autentiseraren kontrollerar värdet klienten skickar genom att utföra samma envägs hash funktion och jämföra dessa två värden mot varandra. Om dom är lika så godkänns autentiseringen med ett Success meddelande, men om dom inte stämmer så skickas ett Failure meddelande tillbaka och anslutningen avslutas.

4. Med ett slumpat tidsintervall görs punkt 1-3 om under hela anslutnings tiden.

Den envägsfunktion som används tillsammans med CHAP är MD5. Hash värdet räknas fram i MD5 med hjälp av ett det Challenge värde som skickas med i Challenge paketet och det lösenord som parterna har gemensamt. Challenge värdet är unikt och oförutsägbart, detta hjälper till att skydda mot återspelningsattacker. Attacker som återupprepar en anslutning med hjälp av paket från en föregående anslutning som den snappat upp genom paket sniffning. Då Challenge värdet ändras varje gång ett nytt Challenge meddelande skickas så blir en sådan attack verkningslös.

Ett CHAP-paket består av 3 fält som alltid finns med. Dessa fält är: Code-fältet där koden talar om vilken typ av CHAP-meddelande som skickas, identification (ID) fältet som talar om vilket nummer paketet har så det går att matcha mot rätt paket och Length fältet som talar om hur stort hela paketet är. Sedan kommer data fältet som i exemplet nedan representeras av dom 3 sista kolumnerna. Beroende på vilken typ av paket som skickas så ser data fältet annorlunda ut. Vid ett Challenge eller Response meddelande består datafältet av 3 fält, ett längd fält som talar om hur långt värde fältet är. Sedan kommer värde fältet som innehåller Challenge- eller Response-värdet. Sist kommer ett namn-fält som innehåller information om det sändande systemet. Skillnaden mellan ett Success- och ett Failure-paket är att dessa innehåller enbart ett meddelande-fält i datadelen. Meddelande fältets innehåll styrs av den implementation av CHAP som för tillfället används, det rekommenderade är att det ska innehålla läsbar data för en människa dvs. ASCII tecken från 32 till 126 decimalt.

Tabell 3, visar dom 4 olika CHAP meddelandena [18].

Typ av paket	1 Byte	1 Byte	2 Bytes	1 Byte	Variable	Variable
Challenge	Code = 1	ID	Length	Challenge Lenght	Challenge Value	Name
Response	Code = 2	ID	Length	Response Length	Response Value	Name
Success	Code = 3	ID	Length		Message	
Failure	Code = 4	ID	Length		Message	

CHAP-paketet läggs sedan in i data fältet i ett PPP-paket och har hexadecimalt C223 som protokollkod.

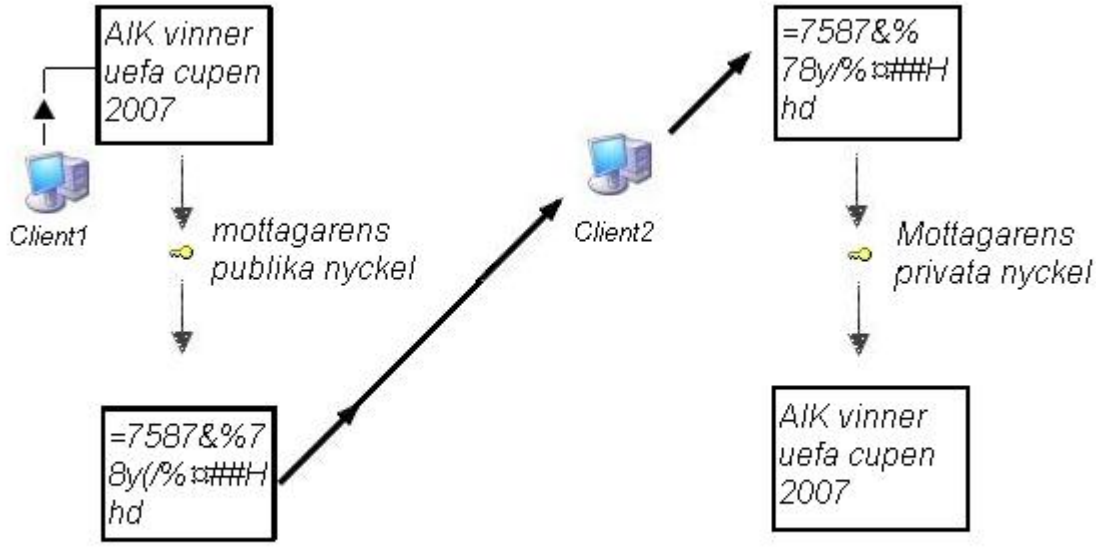
Källa: [19].

2.7 Krypterings terminologi

När man sätter upp ett VPN är säkerhet en av de viktigaste aspekterna. För att åstadkomma säkerhet använder man sig av kryptering. För att kunna kryptera använder man sig av kryptografiska algoritmer som inte är annat än matematiska funktioner. Vanligtvis består dessa funktioner av två samhörande funktioner, en för kryptering och en för dekryptering. För att kunna kryptera ett paket med hjälp av en kryptografisk algoritm används idag nästan alltid nycklar. Detta gör att det inte spelar någon roll om en hackare känner till algoritmen du använder. Om hackaren inte vet din nyckel så kan han inte läsa ditt krypterade meddelande. De kryptografiska algoritmerna kan delas in i två kategorier symmetriska och asymmetriska.

2.7.1 Asymmetrisk Kryptering

Vid denna kryptering används samma krypteringsalgoritm men med olika nycklar för krypteringen och dekrypteringen. Vid denna typ av kryptering används ett matchande nyckelpar som kallas publik och privat nyckel. I en kommunikation använder sändaren av ett meddelande motpartens publika nyckel för att kryptera information avsett för denna. Motparten använder sedan sin privata nyckel för att dekryptera denna information. Därför är det viktigt att den privata nyckeln hålls hemlig vid asymmetrisk kryptering.



Figur 25 Ett exempel på kryptering med en publik nyckel och sedan dekryptering med en privat.

I bilden ovan (Figur 25) visas ett exempel på denna process. Client1 som är den sändande parten krypterar sitt meddelande med mottagarens publika nyckel och vet att bara den som innehar den matchande privata nyckeln kan dekryptera meddelandet. Vanligtvis förvaras privata nycklar på den lokala hårddisken men den kan också förvaras på andra sätt. Ett exempel på detta är så kallade smartcard. De publika nycklarna tillhandahålls och distribueras vanligtvis via en katalogtjänst som till exempel Microsofts Active Directory (AD) .

De mest kända krypteringsalgoritmerna för denna typ av kryptering är DH, ElGamal och RSA (Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman). Dessa algoritmer används sällan för kryptering av data då de är alldeles för långsamma, de används istället för att lösa problemet med nyckeldistribution för symmetriska krypteringsalgoritmer.

2.7.1.1 Diffie Hellman nyckel utbyte (DH)

Diffe-Hellman protokollet uppfanns 1976 av Whitfield Diffe och Martin Hellman. Protokollet tillåter två kommunicerande parter att generera en delad hemlighet och kommunicera över ett osäkert nätverk som Internet. Nedan följer ett exempel på hur detta kan fungera.

$$\mathbf{C = A^X \ (MOD \ B)} \qquad \mathbf{(1.)}$$

Ovan har vi den funktion som används i DH, där A är ett utav talen parterna förhandlar fram, x är det tal de enskilt väljer och B är det andra talet de förhandlar fram gemensamt. MOD står för Modulus och innebär att resten vid heltalsdivision blir svaret. Till exempel så blir 11/2 = 5,5 men om man istället bara använder heltal så blir 11/2 = 5 med resten 1.Det modulus gör är den ger ut resten som svar. Då blir 11 MOD 2 = 1.

Det börjar med att de båda parterna bestämmer de två talen A och B. Dessa två tal A och B skapar en envägsfunktion, där A skall vara minde än B. I vårt exempel kommer parterna fram till A = 6 och B = 11. Envägsfunktionen blir således.

$$C = 6^x \text{ (MOD 11)} \quad (2.)$$

Efter detta väljer de kommunicerande parterna varsitt eget tal som de håller hemligt. I vårt exempel så skall host1 och host2 kommunicera. De kom fram till ovanstående envägsfunktion och väljer efter det dessa tal individuellt.

Host1 = 5

Host2 = 12

Dessa tal sätter de in i envägsfunktionen.

$$\text{Host1} \rightarrow 6^5 \text{ (MOD 11)} = 10 \quad (3.)$$

$$\text{Host2} \rightarrow 6^{12} \text{ (MOD 11)} = 3 \quad (4.)$$

I nästa steg talar de om för varandra vad de fick för värde. Nu sätter de in den andre partens svar i sin envägsfunktion istället för talet A.

$$\text{Host1} \rightarrow 3^5 \text{ (MOD 11)} = 1 \quad (5.)$$

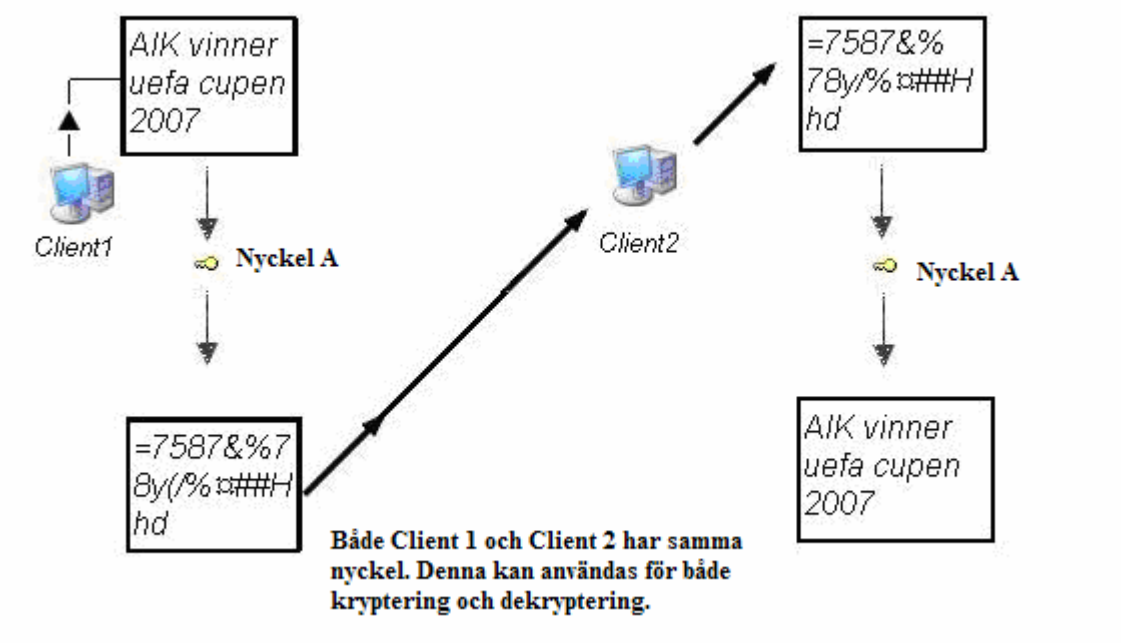
$$\text{Host2} \rightarrow 10^{12} \text{ (MOD 11)} = 1 \quad (6.)$$

Båda kommer alltså att få samma tal.

DH bygger på att man inte kan räkna baklänges. En hackare kan se vilken envägsfunktion som används mellan Host1 och Host2. De kan också sniffa upp de två värdena som parterna skickar till varandra. Detta räcker dock inte för att komma fram till de båda parternas hemliga tal. För att denna metod ska bli säker och svår att knäcka med hjälp av till exempel en brute force attack används mycket större tal än i detta exempel. Använder man sig till exempel av en 56 bitars nyckel betyder det att man använder tal mellan 0 och 2^{56} vilket totalt blir 72057594037927936 olika kombinationer.

2.7.2 Symmetrisk kryptering

Symmetrisk kryptering baseras på att sändaren och mottagaren delar en och samma nyckel (se Figur 26). Denna nyckel kan användas för att kryptera och dekryptera data parterna emellan. Största problemet med denna lösning är att hitta ett sätt att distribuera nycklarna mellan parterna på ett säkert sätt. Idag brukar det innebära att administratörer får springa runt och sätta nycklar på datorer som skall kommunicera säkert, det är förståss ingen hållbar lösning i en större organisation. Vanliga symmetriska krypteringsalgoritmer är DES, TDES och AES. Symmetriska och asymmetriska krypteringsalgoritmer används ofta tillsammans. Så är exempelvis fallet i IPSec där en asymmetrisk krypteringsalgoritm vanligtvis DH används för att på ett säkert sätt utbyta en nyckel och när denna nyckel är förhandlad tar DES eller TDES vid för krypteringen av data.



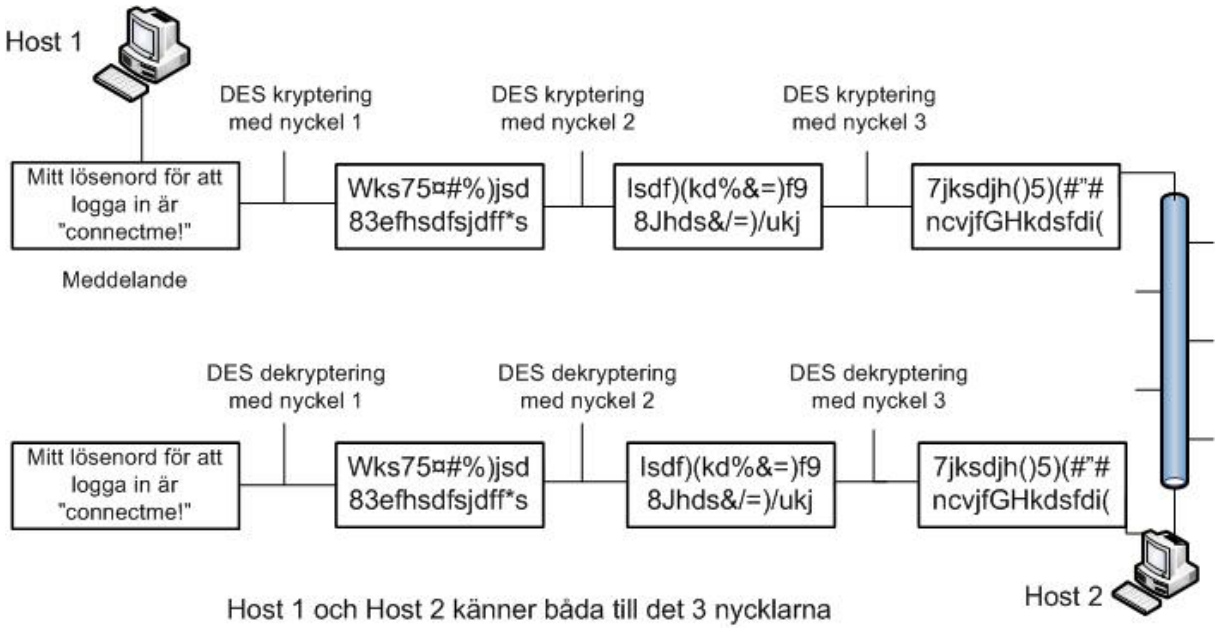
Figur 26 Ett exempel på kryptering och dekryptering då båda parter har samma nyckel.

2.7.2.1 DES och 3DES

DES (Data Encryption Standard) är som sagt en symmetrisk krypteringsalgoritm vilket alltså innebär att den använder samma nyckel för kryptering och dekryptering. DES är ett så kallat blockchiffer. Blockchiffer krypterar texterna i omgångar eller block. I DES är ett block 64 bitar, detta innebär att både chiffertexten och det riktiga meddelandet kommer vara lika långt, 64 bitar. Man krypterar alltså 64 bitar i taget av ett meddelande. Detta meddelande krypteras genom att en algoritm utför ett antal matematiska funktioner på det ursprungliga meddelandet tillsammans med den gemensamma nyckeln och på så sätt krypterar det.

Nyckeln som DES använder för kryptering är en 56 bitars nyckel vilket innebär att ett meddelande kan krypteras på 2^{56} = 72057594037927936 olika sätt. Detta kan tyckas ganska mycket, men den har blivit knäckt. Vid universitetet i Bochum och Kiel i Tyskland har de byggt en dator för runt 10000 dollar som genom Brute Force kan knäcka DES på mindre tid än en vecka. För att förbättra DES skapades 3DES eller TDES som det också kallas (Triple Data Encryption Standard). Denna är vanligare än DES idag eftersom den erbjuder större säkerhet. TDES använder samma matematiska algoritm som DES men i TDES används 2 eller 3 nycklar istället för en beroende på vilket läge man vill använda.

Varianten där man använder 3 nycklar kallas 3-key TDES och krypterar helt enkelt ett meddelande 3 gånger med hjälp av 3 olika nycklar. Enligt formeln DES(key_3;DES(key_2;DES(key_1;*Message*))). I Figur 27 visas detta.



Figur 27 Illustrerar hur en kryptering och dekryptering går till med 3 nycklar i TDES.

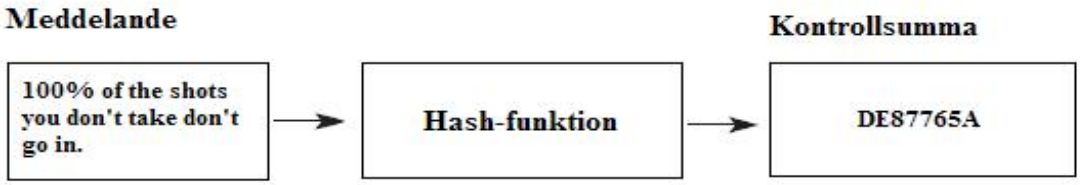
Den andra variant där två nycklar används kallas 2-key TDES. Kortfattat fungerar det så att sändaren först krypterar ett meddelande, på liknande sätt som DES gör med en av nycklarna. Sedan dekrypterar sändaren samma block med den andra nyckeln, denna andra så kallade dekryptering av meddelandet kommer inte att återskapa ursprungsmeddelandet eftersom en annan nyckel används, detta fungerar istället som en slags kryptering. Till sist krypterar sändaren återigen meddelandet med den första nyckeln och skickar iväg det. Formeln för denna metod blir $DES(key_3;DES^{-1}(key_2;DES(key_1;Message)))$.

Oavsett vilken variant av TDES man använder så kommer meddelandet att bli svårare att dekryptera eftersom nyckellängden ökar. I 2-key TDES är nyckellängden 112 bitar och i 3-key TDES är nyckellängden 168 bitar. Dekrypteringen i DES sker på samma sätt som krypteringen men naturligtvis i motsatt ordning. För noggrannare teknisk information om hur DES krypterar samt dekrypterar läs [20], [21],

Övriga källor kryptografi: [22],[9]

2.7.3 Hash-funktioner

När två parter skickar meddelanden till varandra vill man vara säker på att informationen som skickas inte ändras på vägen. För att säkra informationen använder man hashfunktioner som skapar så kallade kryptografiska kontrollsummor. Meddelandet som sändaren vill skicka körs genom hashfunktionen som skapar denna kontrollsumma eller fingeravtryck av paketet. Summan krypteras vanligen innan den skickas med hjälp av en hemlig nyckel parterna emellan, det gör att sändaren autentiseras, alltså kan bara legitima användare sända och ta emot paket till varandra. Mottagaren tar sedan emot paketet dekrypterar det och beräknar sedan också en kontrollsumma av paketet med hjälp av samma hashfunktion som sändaren använde. Om mottagarens och sändarens kontrollsummor är samma kan mottagaren anta att paketet är orört och accepteras, om kontrollsumman inte stämmer med sändaren, kommer det att kastas.



Figur 28 Visar hur ett meddelande kan se ut efter en Hash-funktion.

Vad en hashfunktion gör är alltså att skapa ett unikt värde för meddelandet, detta värde är mycket kortare än själva meddelandet och skall ha en bestämd längd. Viktiga egenskaper i en bra hashfunktion är att det skall vara omöjligt att utifrån den kryptografiska kontrollsumman återskapa meddelandet och att två meddelanden inte skall kunna generera samma hashvärde. Tanken med en hashfunktion är att det skall vara lätt att beräkna ett hashvärde utifrån ett meddelande men omöjligt att beräkna meddelandet utifrån hashvärdet. De två vanligaste hashfunktionerna idag är Message Digest 5 (MD5) och Secure Hash Algorithm (SHA). SHA1 är den som oftast används, den genererar en kontrollsumma på 160 bitar medan MD5 ger ett värde på 128 bitar. Detta gör SHA1 något säkrare men också något långsammare än MD5. Men man bör ha i åtanke att både MD5 och SHA1 har blivit knäckta. Ett sätt att komma ifrån detta är att salta lösenordet innan det körs genom Hash-funktionen.

Källa:[23]

2.8 Certifikat och Public Key Infrastructure

Vi har i tidigare kapitel (2.7.1) beskrivit asymmetrisk kryptering där parterna som vill kommunicera säkert använder sig av en publik och en privat nyckel för att kryptera samt dekryptera information. Tanken med denna teknik är att man känner till den mottagande partens publika nyckel och krypterar informationen man vill sända med denna. Motparten kan sedan dekryptera informationen med hjälp av sin egna privata nyckel. Det finns dock vissa problem med denna metod. Tänk dig följande exempel där Nils och Joakim vill skicka information till varandra, och Richard som i exemplet är en hacker lyssnar på trafiken. Joakim och Nils kommer först att byta publika nycklar. Detta sker i klartext och Richard kan sniffa upp de båda nycklarna. Detta borde vid första anblick inte vara ett problem eftersom att den publika nyckeln bara kan användas för att kryptera information och inte dekryptera den. Eftersom man använder sig av starka krypteringsalgoritmer ska det heller inte finnas nått sätt för Richard att lista ut den privata nyckeln med hjälp av den publika. Det finns dock problem med att i klartext skicka publika nycklar. En hackare kan utnyttja detta med hjälp av en så kallad man-in-the-middle-attack. Om Richard går in och kapar kommunikationen och på så vis låtsas vara Nils kan han eftersom han vet Joakims publika nyckel skicka krypterade meddelanden till Joakim. Problemet med denna metod är att Joakim tror sig prata med Nils men kommunicerar i själva verket med Richard. För att komma tillrätta med detta problem har man skapat PKI (Public Key Infrastructure). En PKI har följande egenskaper:

- Autentiserar och registrerar ändpunkter som skall kommunicera säkert
- Verifierar integriteten hos publika nycklar
- Autentiserar förfrågningar av publika nycklar samt sparar dem på ett säkert sätt
- Skapar certfikat
- Tar bort ogiltiga publika nycklar

PKI hjälper oss att på ett säkert sätt distribuera publika nycklar till autentiserade användare. För att göra detta använder sig PKI av certifikat. Certifikat skapas av en CA (Certificate Authority) som är en hörnsten i PKI. Det första som händer vi skapandet av ett certfikat till en enhet är att enheten registrerar sig hos CA:n. Den talar om sin identitet och autentiseras på så vis hos CA:n. Om autentiseringen lyckas kommer CA:n att utfärda sin publika nyckel till enheten. Alla autentiserade användare kommer alltså ha tillgång till CA:ns publika nyckel. När detta steg är gjort kommer enheten att skapa ett asymmetriskt nyckelpar. När detta är skapat kommer enheten att skicka sin publika nyckel till CA:n. När CA:n får den publika nyckeln signeras denna med CA:ns privata nyckel och skapar sedan ett certifikat till denna enhet. Detta kommer att innebära att om en annan ändpunkt skall kunna kryptera meddelanden till denna enhet måste den också ha tillgång till CA:ns publika nyckel och för att ha tillgång till denna måste den vara autentiserad av CA:n. Detta bidrar till att bara autentiserade enheter kan få tillgång till publika nycklar. CA:n kommer alltså att fungera som en betrodd tredje part i kommunikationen.

Vi har pratat om enheter som får certifikat utfärdade, vilka är då dessa enheter som behöver certifikat? I VPN sammanhang används certifikat ofta för att på ett säkert sätt autentisera VPN gateways och användare för varandra.

2.9 Autentisering av användare

För att kontrollera vilka som får logga in på systemet och med vilka behörigheter använder man sig ofta av en Accounting, Authorization och Authentication (AAA) server. Denna ger precis som namnet antyder åtkomst och behörighet till system, samt central loggning. En av anledningarna till att man gör detta är för att centralisera administrationen. Har man till exempel flera accesservrar kan det vara smidigt att binda ihop dessa till en och samma AAA-server. AAA kan exempelvis sköta användare autentisering vid uppringda sessioner mot olika databaser, som till exempel Active Directory. Den kan specificera detaljerad sessionskonfiguration för varje användare samt ge stöd för ett centraliserat accounting system. En annan orsak till att AAA-servrar används är att den utrustning man ringer upp ofta är begränsad rent hårdvarumässigt, har till exempel. inte tillräckligt med minne för att spara alla användare lokalt. En AAA-server kan även kallas Remote Authentication Dial In User Service (RADIUS) server eftersom RADIUS är det protokoll som sköter ovanstående funktioner. Ett annat protokoll som är likt RADIUS är Terminal Access Controller Access-Control System (TACACS+). Vi har i vårt arbete använt oss av RADIUS så därför går vi in på det lite noggrannare.

2.9.1 RADIUS

RADIUS-protokollet är öppen standard vilket har gjort att många fjärraccesspunkter stödjer det. RADIUS fungerar som ett klient/server system. De olika accesspunkterna är så kallade RADIUS-klienter som frågar en RADIUS-server om användaren är giltig och vilken behörighet denne har. Här nedan visas hur det går till när en RADIUS-klient gör en förfrågan till RADIUS-servern.

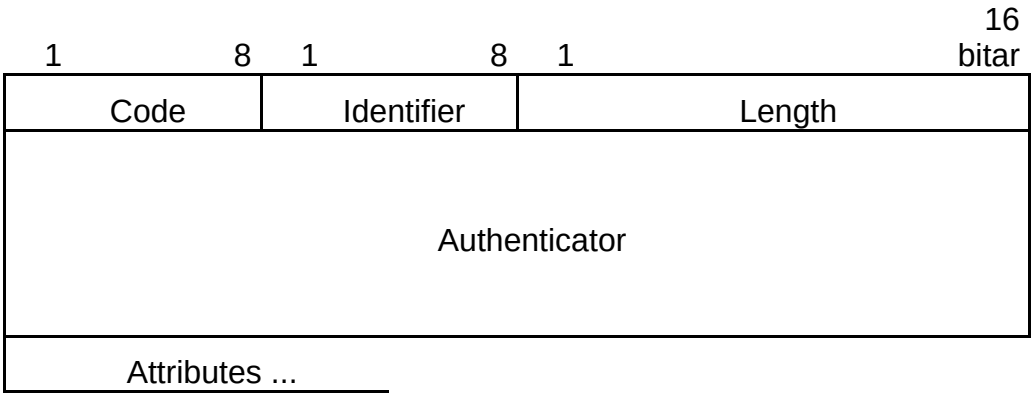
- RADIUS-klienten skickar ett **Access-Request** paket med användarens användarnamn, det krypterade lösenordet, RADIUS-klientens IP-adress och portnummer till RADIUS-servern. RADIUS-servern stödjer flera olika autentiseringsmetoder såsom Password Authentication Protocol (PAP), CHAP och UNIX login.

- RADIUS-servern letar igenom sin databas efter användarnamnet, om det inte finns med kan en standard profil användas eller så svarar den direkt med ett **Access-Reject**. Access-Reject meddelandet kan följas av ett felmeddelande som talar om orsaken till nekandet. När användarnamnet finns i databasen och lösenordet stämmer så svarar RADIUS-servern med ett **Access-Accept** paket där attributen för anslutningen skickas med. Vanliga parametrar är service typ (shell eller framed), protokoll typ, en IP adress att tilldela klienten (statisk eller dynamisk), en behörighetslista eller en statisk route för RADIUS-klientens routing tabell.

- RADIUS-klienten agerar gentemot svaret och parametrarna i det.

Ett RADIUS-paket kapslas in i ett UDP-paket. De portar som används är 1812 för autentisering och behörighetskontroll och 1813 för kontohantering. Kontohantering kan användas separat och används till exempel för att mäta hur mycket resurser en klient använder under en session. Då kollar man det första paketet och det sista paketet i sessionen och läser av de paketen för att få fram tid, antal paket, bytes osv. som skickats.

Ett RADIUS paket ser ut som nedan (Figur 29):



Figur 29 Visar strukturen hos ett RADIUS paket.

Code-fältet är 1 byte långt och talar om vilken typ av RADIUS-paket som skickas. De koder som finns är följande:

1 Access-Request **2** Access-Accept **3** Access-Reject **4** Accounting-Request **5** Accounting-Response **11** Access-Challenge **12** Status-Server **13** Status-Client **255** Reserved.

Paket med koderna **4** och **5** skickas till port 1813 för accounting istället för port 1812 som de andra skickas till. Om RADIUS-servern tar emot ett paket med felaktig kod slängs det omedelbart.

Identifier-fältet är som Code-fältet också 1 byte långt. Det innehåller ett sekvensnummer som används av RADIUS-klienten för att matcha ett RADIUS-svar mot rätt förfrågan.

Length-fältet är 2 byte långt och talar om hur stort hela paketet är inklusive alla fälten.

Authenticator-fältet är 16 byte stort. Detta används av klienten för att kontrollera äktheten i RADIUS-serverns svar och av RADIUS-servern för att gömma lösenord.

Attribute-fältet innehåller 3 olika fält i sig:

- Attribute-type 1 byte långt. Talar om vilket värde som skickas(Se lista i De olika Attribute värdena i ett RADIUS paket).
- Length visar längden av alla attribute-fälten tillsammans. Är 1 byte långt.
- Value-fältet är mellan 0 och 253 byte långt beroende på värdet som skickas. Det finns 4 olika värdetyper:

  1 Sträng 0-253 byte

  2 Adress 4 byte mest signifikanta byten först

  3 Integer 4 byte mest signifikanta byten först

  4 tid 4 byte där första byten även den mest signifikanta innehåller antalet sekunder från 1/1/70.

Källa: [24].

2.10 NAT-Traversal (NAT-T)

NAT-T är en standard som skapades för att möjliggöra IPSec kommunikation genom en NAT-router. En NAT-router är idag mycket vanlig då de flesta hushållen som använder Internet ofta har mer än en dator, men man får oftast bara en publik IP-adress från ISP'n. För att alla datorer skall få tillgång till Internet har man en NAT-router som tilldelas den publika IP-adressen och sedan delar ut privata IP-adresser till de datorer som är kopplade till den. För att datorerna med en privat IP-adress skall kunna kommunicera med datorer/tjänster ute på Internet så krävs det att paketen som skickas ut mot Internet får en publik IP-adress som avsändaradress. Utan en publik IP-adress som avsändaradress kommer mottagaren aldrig kunna svara. Det är Just detta som NAT-funktionen löser. I paketen som skickas byter den ut den privata IP-adressen i avsändarfältet mot den publika IP-adressen som den fått från ISP'n. När det sedan kommer ett svar på det paketet så har NAT-routern en lista på vilka paket den har skickat och kan då se vilken privat IP-adress som svaret skall skickas till. Den byter då ut den publika destinations IP-adressen mot den rätta privata IP-adressen och skickar ut paketet på det interna nätverket. På så sätt kan flera datorer i nätverket kommunicera samtidigt mot Internet. För att sedan förstå varför ett IPSec paket inte kan passera genom en NAT-router så måste man ta en titt på vad NAT-

routern gör med IPSec-paketen när dessa passerar. Ett IPSec-paket ser ut som Figur 30 nedan.

IP head-er	IPSec ESP header	*UDP/TCP header*	*L2TP header*	*PPP header*	*PPP Payload*	*IPSec ESP trailer*	IPSec Auth trailer

Figur 30 IPSec paket i Transport mode.

När detta paket passerar genom en NAT-router sker följande saker:

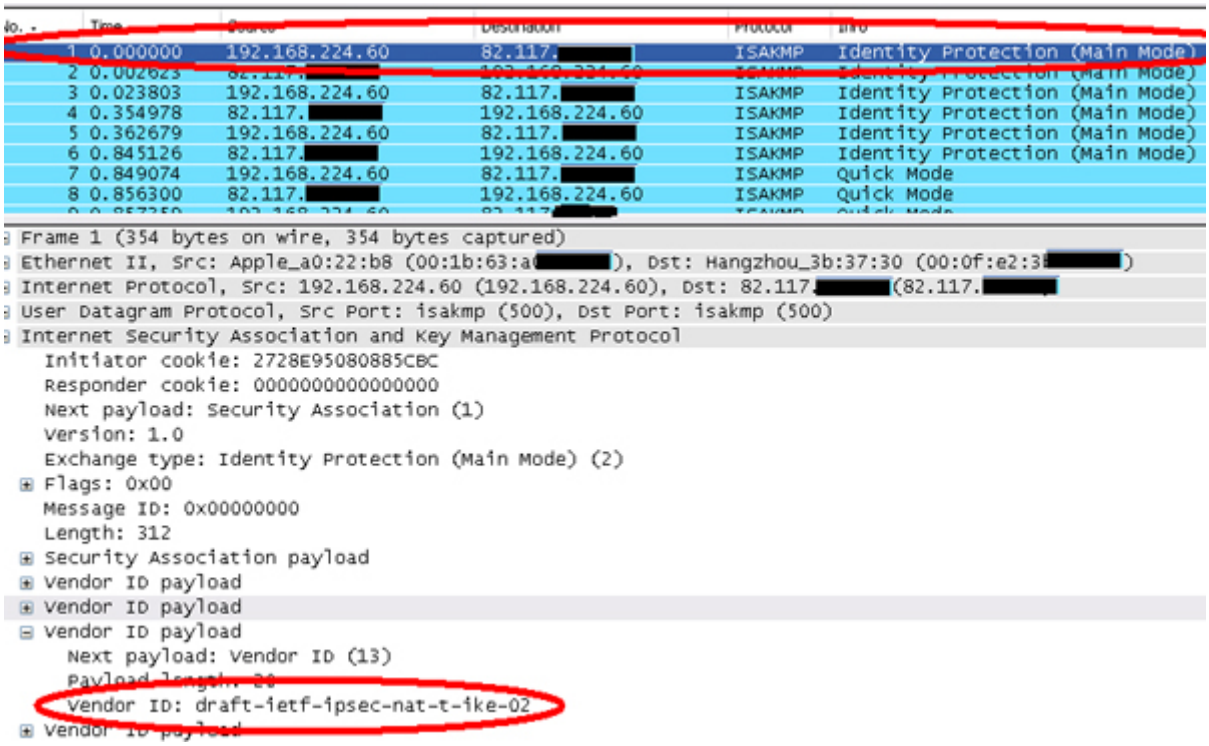
- NAT-routern försöker ändra den kontrollsumma som ligger i UDP-headern, men eftersom denna är krypterad så går inte det. Detta på grund av att NAT-routern ändrar avsändaradressen i paketet när det passerar och denna adress är en av parametrarna som används för att räkna ut kontrollsumman. När paketet då anländer till mottagaren och mottagaren räknar ut kontrollsumman som då inte blir den samma som den i paketet (på grund av den ändrade adressen) så räknas kommunikationen som osäker och paketet slängs.

- NAT-routern kan inte använda UDP-portarna i UDP-headern till att upprätthålla fler än en IPSec-anslutning samtidigt eftersom dessa är krypterade och då inte synliga för NAT-routern. Då kan den alltså inte hålla reda på vilken IPSec-kommunikation som hör till vilken dator.

- Ett annat problem som uppstår när NAT-routern ändrar avsändaradressen är att mottagaren jämför avsändaradressen i pakethuvudet mot en dold adress i identification IKE datafältet. Den adress som ligger i IKE datafältet är den ursprungliga privata avsändaradressen. Då dessa inte kommer stämma överens så tror mottagaren att paketet har blivit ändrat på vägen (vilket det har, men inte får) och slänger detta direkt och avbryta IKE förhandlingen.

Dessa problem löses i och med NAT-T standarden. Det NAT-T gör är att kapsla in ESP-huvudet i ett nytt UDP-huvud som ligger mellan IP-huvudet och ESP-huvudet. Då får man ett huvud som NAT-routern kan läsa av portnummer från för att klara av flera samtidiga anslutningar. NAT-T lägger även till original avsändaradressen (den privata IP-adressen) i ett NAT-OA (Original Address) data fält. Detta löser problemet med att mottagaren inte kan räkna fram en korrekt kontrollsumma och att mottagaren inte kan jämföra den dolda adressen i IKE mot den riktiga avsändaradressen.

För att NAT-T överhuvudtaget skall fungera måste båda parterna stödja NAT-T och ha det aktiverat. Det är under fas 1 i IKE förhandlingen som parterna kan se om dem stödjer NAT-T. Detta syns i Vendor ID data fältet i ISAKMP protokollet (Se Figur 31 nedan)



Figur 31 Visar hur ett ISAKMP paket (övre inringningen) ser ut med NAT-T förhandlingsfältet (den nedre inringningen) t aktiverat. Dom svarta fälten är Confidence IP-adress som vi inte vill lämna ut.

Om båda parterna har skickat med det data fältet som är inringat ovan(Figur 31) så kommer NAT-T att kunna användas. Bara för att det är aktiverat är det inte säkert att det kommer användas. Det används bara om en NAT-router finns någonstans mellan dem. Detekteringen av en NAT-router sker genom att en hash-summa räknas fram från orginaladressen och original portnummret och läggs i datafältet i ett NAT-Discovery (NAT-D) paket. När den andra parten tar emot paketet och räknar ut hash-summan på nytt (från avsändarens adress och portnummer), jämförs de båda hash-summorna. Om de är lika ligger avsändaren inte bakom en NAT-router, men om de är olika så har ju en NAT-router ändrat avsändaradressen och kanske även portnummret. Detta gör båda parterna och på så sätt vet de om det inte finns, eller om det finns en eller två NAT-routrar mellan dem. Den part som sitter bakom en NAT-router måste upprätthålla NAT-routerns NAT-tabell genom att i intervaller skicka Keep-Alive-paket. Intervallet för ett Keep-Alive-paket är som standard satt till 20 sekunder. Dessa paket kommer bara att skickas om det inte skickats något paket till användaren inom den givna intervallen.

Källor: [25], [26].

2.11 Grupp policies

Det finns två olika typer av grupp policies, användar policies som tillämpas när en användare loggar in och dator policies som tillämpas innan inloggningen. Grupp policies kan användas för en mängd olika inställningar i ett Active Directory domän, men vi kommer inte gå in på alla möjligheter de ger i denna uppsats. Vi kommer ge en kortare förklaring i denna avhandling. Exempel på användningsområden för grupp policies kan dock vara uppdatering av klienternas operativsystem, konfiguration av brandvägg, installation av särskild mjukvara, lösenordshantering och mycket mer.

Grupp policies kan tillämpas på flera nivåer i ett AD domän. Man kan till exempel konfigurera ett helt domän eller bara delar av ett domän med olika grupp policies.

Grupp policies erbjuder centraliserad hantering och konfigurering av datorer och användare i ett AD domän. Grupp policy inställningar sparas i så kallade Grupp Policy Objekt (GPO) i AD. Grupp policies kan anges på ett antal olika nivåer: platser, domäner och organisationsenheter (OU). När en domänansluten dator startas kommer de dator policies som är inställda i de GPO som är kopplade till den plats, domän och OU som datorn befinner sig i att tillämpas. Samma sak gäller när en användare loggar in men då tillämpas istället användarprinciperna.

2.11.1 Säkerhet med grupp policies

Grupprinciper används ofta för att öka säkerheten i en miljö. Fördelen med att använda sig av detta är man kan administrera hela sitt system från en central plats och slipper därmed sätta på löparskorna och springa mellan klienter och serverar. Framför allt så vet man också att alla datorer följer organisationens säkerhetspolicy. Nyckeln till att detta ska fungera på ett bra sätt är givetvis en bra OU-struktur. Vissa säkerhets policies vill man ofta ska ligga på alla datorer på ett domän, detta gör man enklast och smidigast genom att sätta en domän policy som alla datorer i domänet måste använda. Sedan kan man på en lägre nivå i våra OU-behållare göra mer definierade säkerhetsinställningar på olika datorkategorier. Vissa av en organisations datorer kanske man vill säkra ytterliggare genom att tvinga dem kommunicera med IPSec, använda strängare brandväggsregler, förhindra installation av program. Andra användare som exempelvis utvecklare på organisationen kanske kräver mer möjligheter i systemet och genom att skapa en vettig OU-struktur så kan man lätt applicera policys på olika grupper. (En guide utförliggare guide hur man strukturera ett domän och applicerar policies finns i bilaga 8 sida 86)

2.11.2 Folder Redirection och Offline files

Folder redirection är en grupp policy i Active Directory som kan sättas på användare i ett domän. Policien ger en administratör möjlighet att omdirigera olika mappar i en användares profil till en delad mapp på en central server. För en användare är detta osynligt. Det ser ut som användaren sparar sina filer i en vanlig lokal mapp men i själva verket så ligger mappen på en annan plats. När en användare eller en applikation behöver tillgång till filer i dessa mappar så blir de automatiskt omdirigerade till denna plats. Man kan inte använda folder redirection på vilka mappar som helst utan bara ett fåtal i användarnas profil. Följande kan omdirigeras.

- Skrivbordet
- Mina dokument
- Start menyn
- Mina bilder
- Application Data

Folder redirection påminner om en annan funktion i Active Directory, Roaming profiles. Roaming profiles är vanligt i till exempel skolmiljöer där man ofta loggar in på olika datorer. I roaming profiles sparas hela användarprofilen på en central plats. Skillnaden mellan roaming profiles och folder redirect är att i roaming profiles så måste hela användarprofilen skickas fram och tillbaka mellan användarens dator och servern varje gång en användare loggar in. I folder redirection skapas en länk till denna server och därför skickas bara den data som användaren behöver. Problemet med att skicka hela profiler är att inloggningstiden blir avsevärt längre, speciellt i de fall som användaren har stora filer i sin profil.

Folder redirection används ofta tillsammans med en annan funktion kallad offline files. Offline files är en metod för att göra nätverksfiler tillgängliga när man inte är ansluten till nätverket. Detta är givetvis användbart för laptop användare som jobbar någonstans där de inte har tillgång till det nätverk där deras filer är sparade. En användare kan med hjälp av offline files arbeta med sina filer som ligger på en otillgänglig nätverksdisk precis som vanligt. När användaren sedan kopplar upp sig mot nätverket igen kommer alla filer som blivit uppdaterade när användaren var offline att synkroniseras mot hur det såg ut senaste gången användaren var uppkopplad och uppdatera dessa till dem ändrade versionerna.

2.12 Åtkomst till Internet under VPN-session

När en användare ansluter till ett företag via en VPN-anslutning så lägger VPN-klienten automatiskt in en ny default-route för utgående trafik och ger den tidigare default-routen ett högre värde eller metric. Enkelt talat innebär detta att all trafik kommer att skickas till vår VPN-gateways IP-adress och alla andra Internet adresser kommer att vara otillgängliga så länge VPN-sessionen är uppkopplad. Många användare vill och behöver kanske vara uppkopplade till Internet samtidigt som de är kopplade till företagets nät via VPN. Innan man tillåter detta bör man noga fundera på om det är absolut nödvändigt att användaren har tillgång till Internet under VPN-sessionen då det kan innebära både prestanda försämringar och säkerhetsrisker. Behöver man tillåta Internet-Access under VPN-sessionen kan man använda en av följande två tekniker.

2.12.1 Split-tunneling

Split-tunneling är en funktion som finns i många VPN klienter som ger möjlighet för en användare som är ansluten till en VPN-session att använda en route för trafiken som är ämnad till VPN och en annan route för övrig trafik, till exempel internetsurfning. Vid användning av split-tunneling så skapas alltså inte en ny default route, som är fallet utan denna funktion, utan istället skapas en ny route med hänsyn till vilken adress som klienten blev tilldelad av VPN-servern. Till exempel om klienten får IP adress (192.168.0.10) vid VPN uppkopplingen så kommer all trafik med destination 192.168.0.0 255.255.255.0 att skickas via VPN-länken. All övrig trafik kommer att skickas via datorns tidigare default-gateway.

Fördelen med denna metod är alltså att användarna kan surfa fritt samtidigt som de använder företagets interna resurser. Nackdelen med split tunneling blir då ganska självklart säkerhetsriskerna. I och med att användaren har vägar till både det publika Internet och ett privat företagsnät. Detta kan vara en säkerhetsrisk om klientens dator är inställd på att tillåta routing eftersom att klienten i dessa fall kan fungera som en gateway

mellan en hackare och ett företags interna nätverk [27]. Måste man använda split-tunneling bör man se till att användarens dator är säker det vill säga att den har brandvägg och antivirus installerat och uppdaterat.

2.12.2 Internet åtkomst via företagets ISP

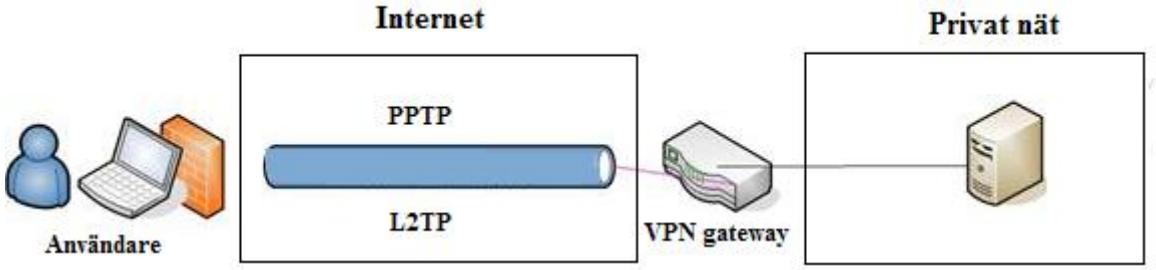
Det andra alternativet som är mycket bättre ur säkerhetssynpunkt är att tillåta Internetåtkomst via det privata nätverket. Detta innebär att Internettrafiken mellan VPN klienten och exempelvis en hemsida går genom företagets brandväggar och eventuell Web-Proxy via VPN-kopplingen. Detta innebär att VPN-kopplingen till företaget kommer att få hantera mycket mer trafik som leder till att företagets WAN-länk kommer att belastas mer. Detta kan få till följd att VPN användarnas sessioner går något långsammare (beroende på uppkopplingens bandbredd). Eftersom användarna på företaget surfar genom företagets ISP så kommer även det att gå långsammare. Fördelarna med denna metod är som sagt säkerhet. VPN-användarnas Internettrafik kan filtreras av en Web-Proxy samt bevakas precis som all lokal trafik i företaget.

3 Mål

Ett utav kraven på vår VPN-lösning var säkerhet. Det finns flera aspekter på säkerhet i VPN. En aspekt är vilka som får tillgång till företagets interna nätverk och vad dessa personer har åtkomst till. En annan aspekt är givetvis att skydda informationen mellan dessa personer och företagets VPN-gateway. Detta görs genom kryptering och autentisering av paketen som går mellan parterna. En sista aspekt är givetvis också att skydda det interna nätverket mot hot som till exempel virus, trojaner och maskar. För att skydda sig mot detta bör man implementera en VPN-policy som sätts beroende på vilken säkerhet man eftersträvar. När man sätter upp ett VPN för användarna är det därför viktigt att planera och se över vad man behöver skydda och hur säker VPN-miljön man implementerar skall vara. I vissa fall bidrar stark säkerhet till försämrad användarvänlighet och kan bli en kostnadsfråga då dyr utrustning måste inhandlas. Till exempel kanske man i säkerhetspolicyn vill att varje anställd ska ansluta från en av företaget säkrad jobbdator, vilket betyder att varje användare måste ha tillgång till en jobbdator. Ett annat exempel kan vara att man vill att en användares dator skall säkras genom vissa skript som kollar att antivirusprogram är installerat och uppdaterat samt att en brandvägg är installerad och konfigurerad på ett visst sätt. Om användarens dator möter de krav som finns får de tillgång till VPN-tjänsten. Dessa lösningar kostar givetvis pengar och kommer att bidra till att användare nekas ansluta då de inte uppfyller kraven. När man implementerar ett VPN bör man därför tänka på följande tre saker, kostnad, säkerhet och användarvänlighet. I vår lösning hade vi inte speciellt mycket ekonomiska medel vilket innebar att vi fick lätta lite på säkerheten för att få till en fungerande lösning med den utrustning som fanns till vårt förfogande.

3.1 VPN-Protokoll

När det gällde VPN-protokoll så gav vår VPN-gateway oss två möjligheter, L2TP/IPSec eller PPTP.



Figur 32, valet stod mellan PPTP eller L2TP /IPSec

Efter att ha testat dessa så kom vi snabbt fram till att L2TP/IPSec skulle passa in på vår kravbild med fokus på säkerhet. Fördelen med PPTP är att det är väldigt enkelt att konfigurera och protokollet har inga problem att klara NAT. Problemet med PPTP är säkerheten. Exempelvis så används bara användarautentisering till skillnad från L2TP/IPSec som både använder sig av användar- och datorautentisering. Denna användarautensering i PPTP är också svag speciellt vid använde av CHAP [28], [29] vilket är en stor svaghet i protokollet. PPTP saknar också andra säkerhetsfunktioner som

L2TP/IPSec har, till exempel skydd mot återspelningsattacker, och data integritet. L2TP/IPSec använder sig också av en starkare krypteringsalgoritm än PPTP.

Problemet med L2TP/IPSec är det inte klarar av NAT vilket innebär problem för användare som sitter bakom NAT. Detta problem kan lösas med en funktion kallad NAT-T som går runt detta problem. Vår VPN gateway stödjer NAT-T vilket innebar att L2TP/IPSec blev ett givet val av VPN-protokoll.

3.2 NAT-T

Som det beskrivits tidigare har de flesta personer idag en bredbandsuppkoppling i hemmet. Med dagens brist på IPv 4 (IP version 4) adresser så fungerar det ofta så att bredbandsleverantören bara ger kunden en unik publik IP adress. För att kunden då skall kunna ansluta mer än en dator åt gången till Internet krävs det en router med NAT funktion (Se avsnitt **2.10 NAT-T)** Utan NAT-T fungerar det då inte att ansluta sig med L2TP/IPSec. För att kunna skapa en VPN-anslutning utan NAT-T krävs det då att klientdatorn har en publik IP-adress. Det innebär att det i många situationer skulle vara omöjligt att använda sig av VPN-anslutningen vill. Sådana situationer är när man själv inte har någon kontroll på nätverket man ansluter sig till Internet via. Det skulle kunna vara om man är på besök hos en kund och lånar en uppkoppling genom deras interna nätverk, sitter på ett hotell eller på ett tåg och får en privat IP-adress. Några exempel på när det skulle fungera utan NAT-T är om man använder sig av ett så kallat 3G (tredje generationens mobilnät) eller GPRS (General Packet Radio Service) modem eller om man kan ansluta datorn direkt till modemet hemma och använda den publika IP-adress man får av ISP'n. Då det sistnämnda kan kräva viss konfiguration av användarens dator och att man kopplar bort en eventuell router med NAT- funktion leder detta till att inte någon annan i hemmet kan använda Internetuppkopplingen. Allt detta extra arbete bidrar till att VPN-funktionen kommer att användas mindre på grund av lathet eller okunskap.

3.3 Enkelhet för användaren

När man skapar en anslutning till företaget så krävs det att anslutningen skall vara lätt att starta och kräva så lite som möjligt av användaren för att fungera. Därför är det viktigt att ge användaren ett färdigt paket där så mycket som möjligt är förinställt. Helst ska användaren bara behöva öppna upp anslutningen och skriva in sitt användarnamn och lösenord. Detta är ett viktigt mål med vårt arbete på Confidence. Risken för att något blir fel minimeras också när användarna inte behöver göra några inställningar. Då får administratören mindre att göra och användarna kan ägna mer tid åt arbetet. Det bidrar till lägre kostnader och högre effektivitet.

3.4 RADIUS

RADIUS många fördelar gentemot att spara alla användare direkt i brandväggen gör att vi anser att den måste inkluderas i VPN-lösningen. Dessa fördelar spar in en hel del tid och gör det lättare för en administratör att hålla koll på användarna i nätverket. Om man väljer att lägga alla VPN-användare lokalt i routern så krävs det att man måste ändra på två ställen istället för på ett ställe. För användarna kan det innebära att man måste komma ihåg ännu ett lösenord, eller om de har samma lösenord både i AD och i routern så finns det ännu en möjlighet för en obehörig att komma åt ett konto. Utöver detta så ger en inloggning via RADIUS användaren direktåtkomst till sina mappar och filer i nätverket. De behöver alltså bara skriva in sitt lösenord och användarnamn en gång vid tunneluppkopplingen.

3.5 Säkerhet i VPN

När man implementerar VPN på ett företag uppstår det en del säkerhetsfrågor. Eftersom VPN förutsätter att man öppnar sina interna system för kommunikation med omvärlden eller Internet så uppstår flera säkerhetsaspekter som man måste ta hänsyn till. Naturligtvis så bör man se till att kryptera och autentisera trafiken på ett korrekt sätt så att inga obehöriga kan få tillgång till interna system eller avlyssna trafik. När väl trafiken är säkrad så är dock inte alla problem lösta.

Det finns en rad frågeställningar att ta hänsyn till. Generella regler som företag brukar använda sig av är att VPN-användare inte skall spara någon information av vikt lokalt på sin dator. Detta dels för säkerhet om datorn blir stulen och dels med hänsyn till säkerhetskopiering. Om användaren sparar sina filer på företagets server så kommer de förhoppningsvis bli säkerhetskopierade med jämna mellanrum. Detta hjälper i de fall en användares dator kraschar eller informationen av någon anledning försvinner. Grundläggande är också att de datorer som används vid VPN-anslutningar följer företagets säkerhetspolicy, viktigaste av allt är förmodligen att datorn som ansluter har ett antivirus- och brandväggsprogram som förhindrar att det interna nätverket blir smittat av virus.

En rekommendation är att bara tillåta datorer som tillhandahålls av företaget och är installerade med antivirus, brandvägg samt använder företagtes säkerhets policies. Om en användare ansluter från en hemdator som används av resten av familjen så innebär det en höjd säkerhetsrisk. Datorn har kanske inte ett antivirusprogram vilket blir en stor säkerhetsrisk för hela det interna nätverket. Dessutom uppstår det även integritetsproblem. Om flera personer har tillgång till datorn så är det lätt hänt att obehöriga kan läsa information som de inte skall ha tillgång till.

Den rekommenderade lösningen är alltså i de flesta fall att ge VPN-användare en bärbar arbetsdator som uppfyller de krav som företaget har och som bara den personen får använda.

En viktig aspekt är också att inte ge tillgång till mer än nödvändigt. Vissa användare kanske bara behöver komma åt sin egen filmapp medan andra användare kör applikationer mot interna databaser. Ett mål när man implementerar VPN är att inte ge tillgång till mer resurser än absolut nödvändigt.

En detalj som många glömmer för att förbättra säkerheten i VPN är utbildning av användare. Informera om varför vissa regler finns och vad det kan innebära om de inte följs. Det är viktigt att ge användaren information om hur tjänsten skall och inte skall användas. Läs mer om detta i vår bifogade säkerhetspolicy som vi skrev till Confidence International (Se bilaga 5 sida 76).

4 Lösningsalternativ

4.1 L2TP KONFIGURATION

Som beskrivs i L2TP över IPSec avsnitt 2.4.4.1 så använder sig L2TP av IPSec för att göra kommunikationen säker. Det första som sker när en L2TP anslutning upprättas är en så kallad IKE exchange (beskrivet i avsnitt 2.4.2.2). Här sker det IPSec kallar för nyckelutbyte och här sker också dator autentiseringen. Det rekommenderade sättet i L2TP/IPSec för att autentisera datorer för varandra är användning av certifikat (avsnitt 2.4.3.2 och 2.8). Tyvärr så stödjer vår brandvägg inte certifikat vilket innebar att vi fick ta det sämre alternativet pre-shared key. Under fas 1 i nyckelutbytet så använde vi oss av de starkaste algoritmerna som fanns att tillgå, vilka var 3DES (avsnitt 2.7.2.1) för kryptering och SHA1 (avsnitt 2.7.3) för autentisering. Under fas 2 i IKE där det bestäms hur trafiken skall skyddas använder vi oss av ESP (avsnitt 2.4.2.1.2) som erbjuder kryptering och autentisering av data. Vi måste även här ställa in vilka algoritmer vi vill använda för detta och vi använder även här de starkaste algoritmerna, samma som i fas 1 vilka var 3DES och SHA1. I fas 2 måste vi även välja vilket läge vi vill att IPSec skall köra i. Eftersom det är flera användare som skall ansluta måste vi välja transport mode (asvnitt 2.4.2.1).

4.2 Brandväggs Konfiguration

Här kommer en redovisning på de inställningar som krävs i routern för att VPN-tunneln skall fungera.

Först skapar vi en IPSec policy-template som vi döper till **hem**. Varje policy-template kan ha ett värde från 1 – 10000, ett lägre värde ger högre prioritet. Eftersom vi bara har en **hem** template så sätter vi det här värdet till 1. I templaten definierar man vilken IKE-peer konfiguration som skall användas för den här anslutningen och vilken IPSec Proposal som skall användas.

```
#
ipsec policy-template hem 1
 ike-peer homeuser
 proposal home
```

Här under visas IKE peer ”homeuser” som används av **policy-template** hem. Det man talar om i IKE peer läget är vilken form av autentiseringsmetod man ska använda i IKE fas 1. I den här routern kan man bara välja att använda sig av metoden pre-shared key, man bör här välja en så säker nyckel som möjligt (se avsnitt 2.4.3.1 för att se vad som definierar en säker nyckel). Sedan definierar man vilken **ike-proposal** som skall användas, detta görs med ett nummer. Om man vill använda sig av NAT-T så skriver man in det här, vilket vi valde.

```
#
ike peer homeuser
 pre-shared-key “En sträng på 1-127 tecken”
 ike-proposal 1
```

```
 nat traversal
```

I ipsec proposal väljer man vilken form av paket inkapsling (encapsulation-mode) som skall användas. Eftersom vi bara känner till den ena noden i VPN tunneln väljer vi Transport. Sen väljer man även vilket IPSec protokoll som skall användas och dess autentiseringsalgoritm och krypteringsalgoritm i IKE fas 2. Här använder vi ESP protokollet tillsammans med SHA1 och 3DES som autentisering och krypteringsalgoritm.

```
#
ipsec proposal homeuser
 encapsulation-mode transport
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
```

Här under har vi den IKE proposal vi valde i IKE peer. Här ställer man in vilken krypteringsmetod och vilken längd på DH nyckeln (avsnitt 2.7.1.1) man vill använda. Vi använder 3DES och DH group 2 som betyder att nyckeln är 1024 bitar lång.

```
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
```

För att kunna köra göra de inställningar som krävs för en L2TP anslutning måste en L2TP-group skapas. I den gruppen sätter vi parametrarna mandatory-CHAP (avsnitt 2.6), undo tunnel authentication och allow L2TP virtual-template 1. mandatory-CHAP tvingar anslutningen till att använda sig av CHAP för användarautentiseringen. När man kör IPSec tillsammans med L2TP så behöver man inte använda sig av tunnel authentication, därav undo tunnel authentication raden. Som default används tunnel authentication.

```
#
l2tp-group 1
 mandatory-chap
 undo tunnel authentication
 allow l2tp virtual-template 1
```

För att alla som ansluter till routerns Internet interface inte skall behöva använda sig av L2TP/IPSec skapar man ett virtuellt interface som VPN-användarna ansluter sig mot. Här väljer man även vilken krypteringsmetod som skall användas för PPP autentiseringen, i vårt fall fanns det 2 alternativ PAP eller CHAP där vi valde CHAP pga. säkerheten. Som de andra interfacen behöver även det här en IP adress. Här definieras också vilken adress pool som VPN användarna skall få en IP adress från.

```
#
interface Virtual-Template1
 ppp authentication-mode chap
 ip address 172.20.3.1 255.255.255.0
 remote address pool 1
```

Ibland krävs det flera olika inställningar för autentisering av användare. Detta görs genom att skapa olika domäner. I routern finns det default en domän som inte går att ta bort. Utöver den har vi skapat en domän som heter confidence, när användaren skriver in sitt användarnamn i klient programmet följt av ett @ så kommer routern att ta det som står efter @ som domännamnet. Som ett exempel tar vi ”anders@confidence” där kommer routern leta efter confidence och hitta det. i routern så talar man då om vilket autentiserings- och vilket accounting schema som skall användas. Vi vill att våra klienter skall få DNS-adressen till företagets DNS-server, då skriver vi in DNS primary-ip ”IP adress”. Den IP-adress vi använder här är går till Confidence interna DNS-server, då all trafik från klienten går via tunneln in i Confidence nätverk måste vi använda deras lokala DNS-server för namnuppslag. Eftersom vi använder en RADIUS-server för autentiseringen så måste här berättas vilken radius konfiguration som skall användas för just den här domänen. Vår radius konfig heter ”confidence_radius”. Det sista vi gör inom det här domänet är att definiera den IP-adress pool som skall användas av VPN-klienterna. Här väljs ett privat nät som inte utnyttjas av Confidence. Detta är de adresser som klienterna tilldelas för att kunna kommunicera på Confidence interna nätverk.

```
#
 domain default
 domain confidence
  authentication-scheme  test
  accounting-scheme actest
  dns primary-ip  192.168.224.10
  radius-server confidence_radius
  ip pool 1 172.20.3.2  172.20.3.50
```

I domänet så talade vi om vilket accounting och autorisations schema som skulle användas, dessa skapas genom att skriva accounting-sheme ”namnet man vill ha på den” sedan väljer man vilket läge man vill använda, vi kör Radius så det väljer vi här. Authorization scheme skapas på samma sätt och här väljer vi också radius.

```
#
 accounting-scheme default
 accounting-scheme actest
  accounting-mode radius
```

För att kunna använda radius måste man skapa en RADIUS-server template, den döper vi till confidence_radius. I den här definierar vi de inställningar som krävs för att ansluta sig till själva radius servern. En nyckel för autentiseringen mot RADIUS-servern sedan IP-adress och portnummer till RADIUS-servern som sköter autentiseringen respektive accountingen. Med kommandot radius-server retransmit 5 timeout 6 sätter vi den tid i sekunder som gäller för hur länge routern skall vänta med att skicka ett request paket när den inte fått något svar på det första paketet och hur många gånger den ska skicka om paketet innan den väljer att markera den RADIUS servern som onåbar. Dessa värden var rekommenderade att använda av [32].

```
#
radius-server template confidence_radius
```

```
radius-server shared-key “den delade nyckeln”
radius-server authentication 192.168.224.10 1812
radius-server accounting 192.168.224.10 1813
radius-server retransmit 5 timeout 6
undo radius-server user-name domain-included
```

För att routern över huvud taget skall fungera med L2TP måste man aktivera den tjänsten. Det gör man med följande kommando.

```
#
l2tp enable
```

För att börja använda de inställningar vi har gjort måste man skapa en policy som appliceras på det interfacet som anslutningarna kopplas upp mot. Man kan ha flera olika policyn i samma grupp i vårt fall map 1, efter det skriver man in prioriteten för just den här policyn. När en anslutning försöker upprättas mot det interfacet som policyn är knuten till går routern igenom policies i ordningen lägst nummer först för att hitta den som stämmer överens med förfrågningen. Efter prioritetsvärdet kommer isakmp som talar om att förhandlingen ska ske automatiskt, efter det talar man om vilken template som skall användas.

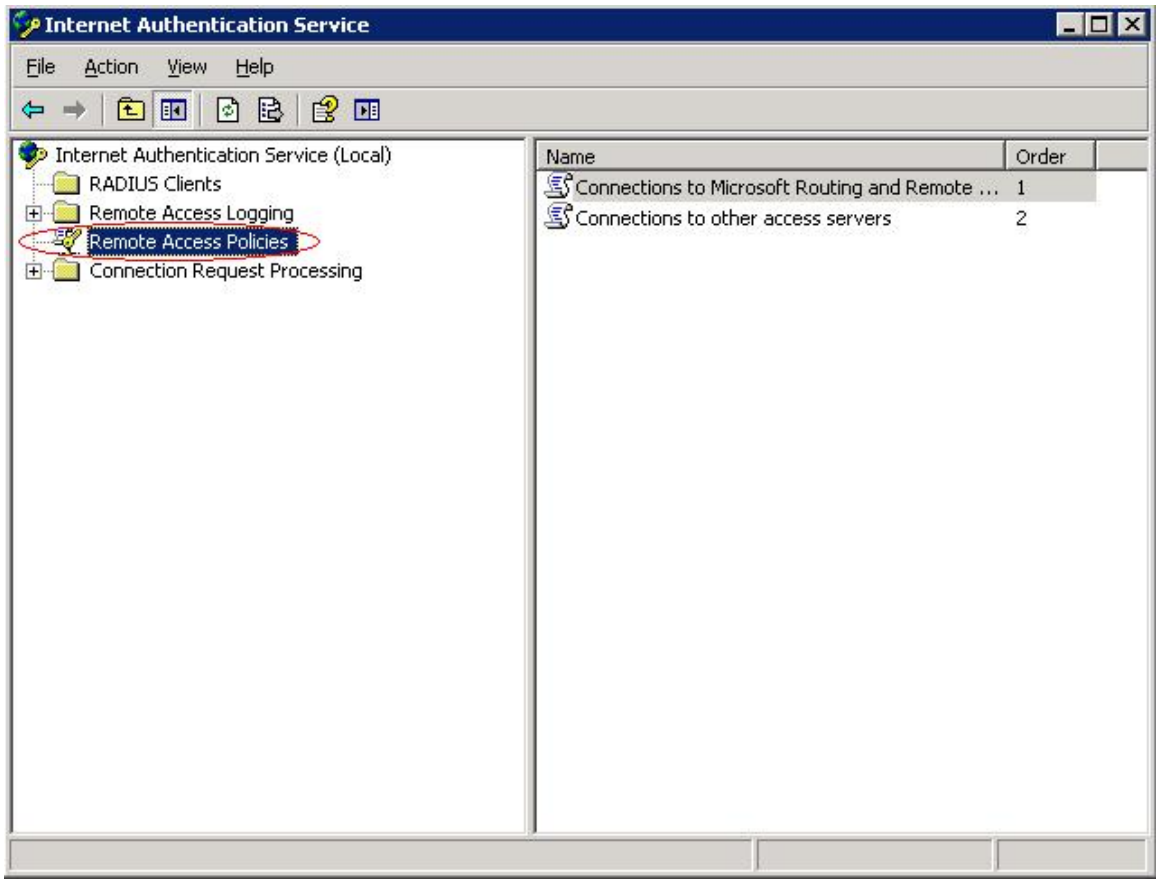
```
#
ipsec policy map1 20 isakmp template hem
```

Det sista vi måste göra för att göra routern helt klar för VPN kommunikationen är att applicera policyn på det interfacet som vi skall ansluta oss till. I vårt fall är det Ethernet interfacet 0/0.

```
#
interface Ethernet0/0
 description Anslutning till Internet
 ip address 82.117.110.2 255.255.255.252
 undo ip fast-forwarding qff
 ipsec policy map1
```

4.3 Policy för fjärranslutning

Som beskrivet tidigare använder vi Mircosofts produkt Internet Authenticatoion Service (IAS) som RADIUS-server, detta för att det som standard ingår i Windows 2003 och för att det är väldigt lätt att integrera med Active Directory. IAS ger oss genom funktionen Remote access policy möjlighet att sätta vilka villkor som ska gälla för att anslutningen skall lyckas. Figur 33 visar var man hittar dessa policies



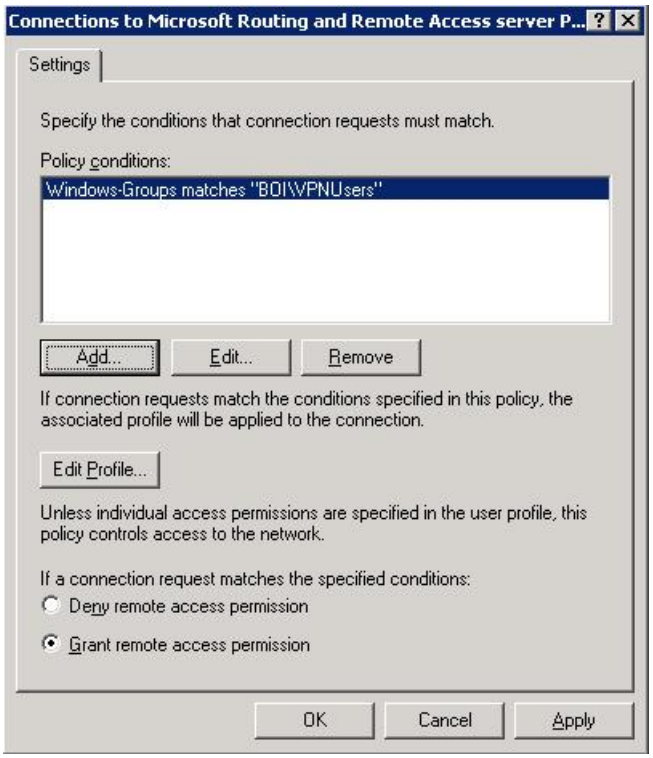
Figur 33 visar vart man hittar Remote Access Policies.

Vi har genom denna funktion möjlighet att sätta en rad villkor som måste uppfyllas för att ge en användare tillgång till företagets VPN. Exempel på villkor som man kan ställa in är:

- Vilka användargrupper som har rätt att ansluta.
- Vilka tunnelprotokoll som får användas.
- Vilka adresser som har rätt att ansluta.
- Hur länge en VPN-session får pågå.
- Vilka autentiseringsmetoder som får användas.
- Hur länge en användare får vara inaktiv innan anslutningen bryts.
- Vilka dagar och tider man får ansluta.

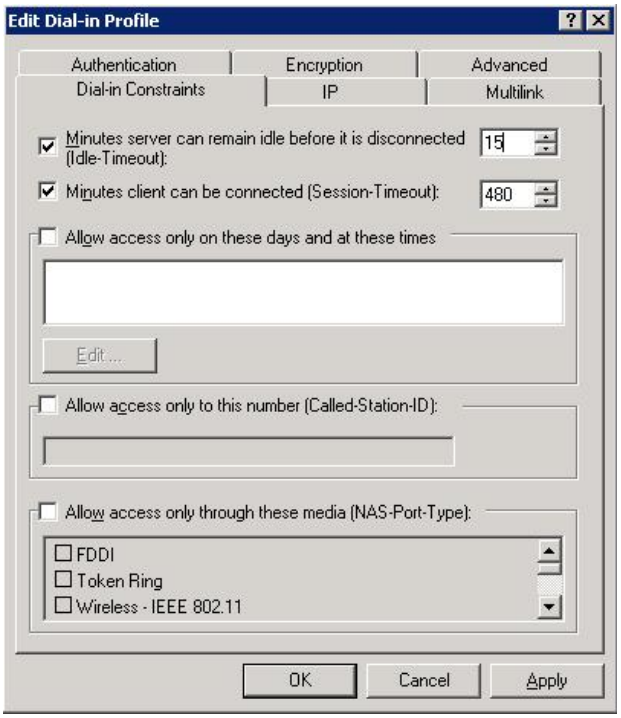
Detta är bara exempel på möjligheter man har för att kontrollera access till företagets VPN. Eftersom det Remote access policy också används i Windows VPN-gateway Routing and Remote Access Service (RRAS) så finns det en mängd inställningar som vi inte behöver bry oss om då vi reglerar vilka protokoll, autentiseringsmetoder samt krypteringsalgoritmer som används i vår brandvägg. Det finns dock en del intressanta inställningar som vi använt oss av.

- Bara användare som tillhör domängruppen VPNUsers har tillgång att ansluta, detta gör att man måste lägga till en användare i denna grupp för att den skall kunna ansluta. Se Figur 34



Figur 34 Visar den inställning i IAS som anger vilka användargrupper som får ansluta.

- Av säkerhetsskäl får en ansluten användare bara vara inaktiv i 15 minuter. När denna tid har gått så bryts användarens anslutning. Användaren får också bara vara uppkopplad i intervaller på 8 timmar. När 8 timmar har passerat måste användaren återigen logga in. Detta är också av säkerhetsskäl i fall någon obehörig av någon anledning skulle komma åt en ansluten dator så skulle denna inställning kunna fungera som en säkerhetsmekanism. Se Figur 35



Figur 35 Visar de inställningar där man begränsar en anslutning till maximalt 8 timmar och inaktivitet till maximalt 15 minuter varefter utloggning sker.

Värt att notera är också att man kan kontrollera vilka dagar och tider som en användare skall få ansluta. Vi har inte applicerat denna policy inställning men det kan vara bra att veta att den finns om man vill neka åtkomst för användare till exempel på helger och kvällar.

4.4 Konfiguration av klientdatorer

När användarna skall upprätta en VPN-anslutning krävs en del konfiguration på deras datorer. Denna konfiguration kan utföras av användarna själva enligt en guide som en administratör tillhandahåller, detta kan ses som riskabelt då fel kan uppstå, samt det faktum att vår pre-shared key på något sätt måste ges till användaren. Ett säkrare alternativ är då att administratören manuellt ställer in en dator med de rätta inställningarna. På så sätt undviker man att vår pre-shared key kommer i orätta händer. Denna metod förhindrar dock inte användarna att gå in och ändra de inställningarna som administratören har ställt in. För att komma undan detta har vi använt oss av ett program som kommer tillsammans med Windows Server 2003 som heter Connection Manager Administration Kit (CMAK). Med CMAK kan man konfigurera en VPN-profil med exakt de inställningar man vill ha och sedan skapa ett installationsprogram som kan köras på klienterna för att installera dessa. CMAK stänger möjligheten för användarna att själva gå in och konfigurera anslutningen vilket naturligtvis är bra. Med hjälp av klara CMAK installationsfiler kan en administratör eller en användare enkelt lägga till en anslutning med ett knapptryck. Ännu bättre är förstås om man kan skapa ett MSI (Microsoft Installer) paket av denna installationsfil och bara skicka ut den till berörda klienter i domänet via en grupp policy i active directory. CMAK ger också andra fördelar till exempel möjligheten att lägga till routes och köra skript på klientdatorn. För mer information om konfiguration av CMAK (Se bilaga 3 sida 67). För att köra L2TP/IPSec så måste de klienterna som ansluter med Microsoft XP ha ett särskilt registervärde. Använder man sig av det paket vi skapat uppdateras registret automatiskt. I de fall där paketet inte kan användas har vi skapat ett skript som kan köras av den som konfigurerar anslutningen. Det registervärde som måste sättas hittas på följande plats.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters\ProhibitIpSec

ProhibitIpSec skall vara satt på 0 och skall så vara för att IPSec skall fungera. För att ställa in så att klienterna kan klara av NAT-T måste man också ändra ett registervärde. Det värdet hittar man på följande plats i registret:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ipsec

Här måste man lägga till följande parameter och en 2a i värde

AssumeUDPEncapsulationContextOnSendRule = 2

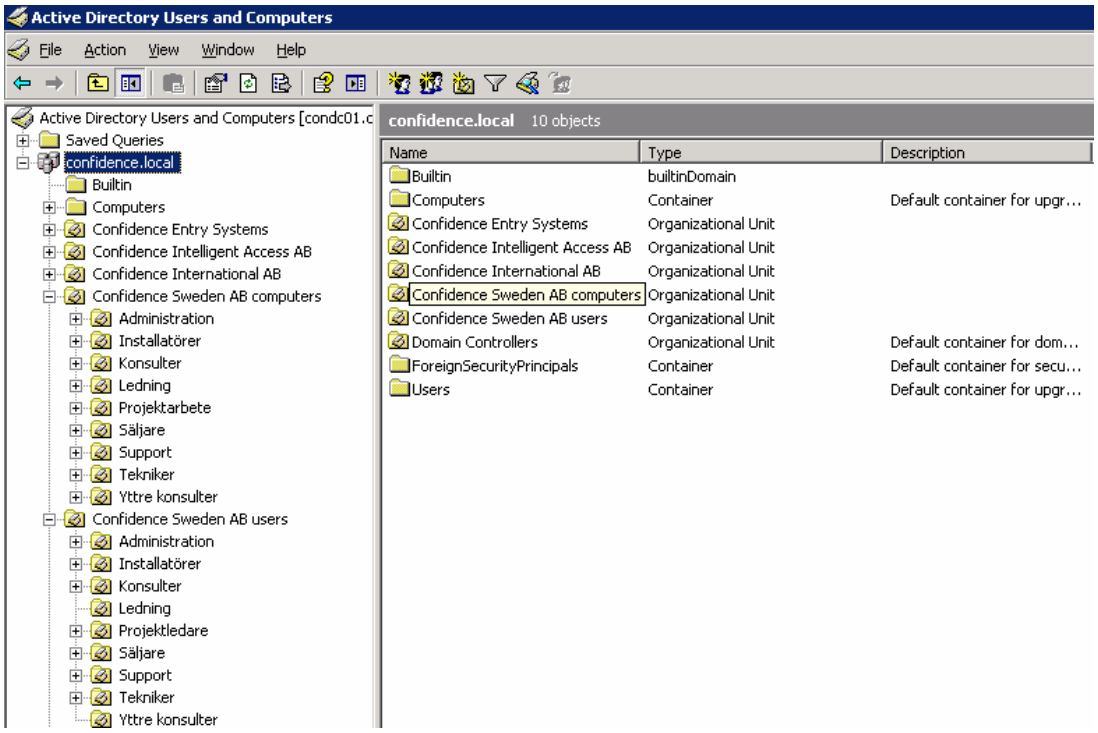
Då vi vill undvika att gå in och ändra dessa värden manuellt i varje klient skapade vi ett skript som tog hand om detta (se bilaga 4 sida 75)

4.5 Grupp Policies

Vår huvuduppgift var att implementera en VPN-lösning till Confidence. Målen som vi har skrivit om tidigare var en användarvänlig lösning men framför allt skulle säkerhet ha högsta prioritet. Både med avseende på att skydda kommunikationen och de interna systemen. Rekommendationen till företaget var att bara använda sig av domänanslutna säkra datorer till kommunikationen med företaget. Fördelen med detta är som det sagts i avsnitt 33 att man slipper virus från oskyddade datorer och i viss grad också ökar skyddet mot att obehöriga personer kan ansluta. En annan fördel med att bara använda just domänanslutna klienter är att man kan tvinga dem att använda domänets säkerhetspolicies vilket gör att man kan öka säkerheten ytterliggare. Dessa grupp policies ger också en rad andra möjligheter som underlättar både distributionen av VPN-klient inställningar samt andra smidiga funktioner som till exempel folder redirect med offline files som beskrivs i avsnitt 2.11.2.

4.6 Säkerhetspolicies

Eftersom företaget nyligen hade införskaffat en ny server som främst skulle fungera som domänkontrollant så var inga säkerhetspolicies konfigurerade i domänet. Vi kom att skapa en rad nya grupp policies för att öka säkerheten hos företaget både med hänseende till VPN-användare och alla lokala användare på företaget. För att kunna göra detta lätt administrerat och tydligt började vi med att skapa en OU-struktur med företagets datorer och anställda indelade i olika avdelningar. Den kom att se ut på följande sätt (Figur 36).



Figur 36 Visar den OU struktur vi skapat i Active Directory.

Alla datorer och användare blev alltså indelade i en OU beroende på vilken avdelning de jobbade på. Detta är en bra grund och gör det lätt att administrera bara vissa grupper av datorer eller användare i framtiden. Till exempel så kanske man i framtiden vill skicka ut ett nytt program till alla tekniker och med denna struktur så kan man enkelt göra detta genom att applicera en software deployment policy på den OU gruppen. Tanken när vi gjorde denna struktur var att företaget skulle kunna använda den för att på ett enkelt sätt kunna sätta policies på olika användargrupper även i framtiden.

Grupp policies används bland annat för att öka säkerheten i en miljö. Fördelen med att använda sig av att detta är man kan administrera hela sitt system från en central plats och slipper därmed sätta på löparskorna och springa mellan klienter och servrar. Framför allt så vet man också att alla datorer följer organisationens säkerhetspolicy. Nyckeln till att detta ska fungera på ett bra sätt är givetvis en bra OU-struktur. Vissa säkerhets policies vill man ofta ska ligga på alla datorer i ett domän, detta gör man enklast och smidigast genom att sätta en domän policy som alla datorer i domänet måste använda. Sedan kan man på en lägre nivå i våra OU-behållare göra mer definierade säkerhetsinställningar på olika dator och användar kategorier. Vissa av en organisations datorer kanske man vill säkra ytterliggare genom att tvinga dem kommunicera med IPSec, använda strängare brandväggsregler, förhindra installation av program osv. Andra användare som till exempel utvecklare på organisationen kanske kräver mer möjligheter på systemet och genom att skapa en vettig OU-struktur så kan man lätt applicera policies på grupper

Vi kom att sätta en rad policies för att öka säkerheten i systemet. Microsoft har en del rekommendationer och så kallade security templates som vi hade mycket nytta av i detta arbete. Dokumentation om dessa kan hittas på [30]

4.7 Säkerhetspolicies i Domänet

Säkerhetspolicies som sätts på domännivå ärvs som beskrivet i bilaga 8 sid 86 vidare till alla OU i domänet. På domännivå läggs säkerhetspolicies som vi vill ska gälla genom hela domänet. Sen kan vi givetvis sätta specifika policies på varje OU, men såvida vi inte gör det så kommer denna princip gälla.

Här är de viktigaste säkerhetspolicies som vi använt på domännivå för användarna i domänet .

Tabell 4, Lösenords policy för Confidence.local

Inställning	Användare
Enforce password history	24 passwords
Maximum password age	90 days
Minimum password age	1 day
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Enforce Password History: Ser till att användare verkligen byter lösenord och inte bara sätter samma lösenord som innan vid lösenordbytet. Inställningen anger hur många nya unika lösenord som användaren måste ha använt innan ett gammalt lösenord kan användas igen.

Maximum Password Age: Används för att ange hur många dagar det måste gå innan användaren måste byta lösenord. Denna policy är viktig eftersom lösenord kan bli knäckta av hackare, komma vilse på olika sätt t.ex. om användarna berättar det för andra eller skriver upp det någonstans så man själv minns det. Med tidsbegränsningen ser man till att användaren regelbundet byter lösenord.

Minimum Password Age: Den här inställningen talar om hur många dagar det måste ha gått innan man får byta lösenordet igen. I vårt fall måste det ha gått minst 1 dag innan man kan byta ett lösenord.

Minimum Password Length: Definierar minsta antal tecken som ett lösenord måste bestå av. Anledningen till att man vill ha ett längre lösenord är för att det blir svårare att knäcka.

Password must meet complexity requirements: När denna är aktiverad måste alla lösenord som skapas eller byts följa en del krav. Standard inställningen är att lösenordet

måste vara minst 6 tecken. Det finns också regler som bestämmer att lösenordet inte får innehålla någon del av användarnamnet. Dessutom finns villkor att användaren måste använda tecken från tre av fyra olika teckenvarianter. Dessa är små bokstäver, stora bokstäver, siffror samt tecken som varken är siffror eller bokstäver. Denna princip är också till för att förhindra att lösenord knäcks. I och med att man använder sig av denna princip ökar antalet möjliga kombinationer på ett lösenord enormt och gör det mycket svårt om inte omöjligt att använda sig av hackertekniker som brute force eller dictionary attacks.

Store password using reversible encryption for all users in the domain: I vanliga fall sparas alla lösenord med en hash algoritm utan anvisning för hur lösenordstexten skall härledas tillbaka från hashen. Man kan med denna inställning använda sig av så kallade omvändbara lösenord. Lösenord som är sparade på detta sätt är svaga och man ska inte använda denna policy om man inte absolut måste. Exempelvis så måste man använda sig av omvändbara lösenord när man använder sig av CHAP genom IAS som var fallet i vår miljö. CHAP måste nämligen kunna läsa lösenordet och inte lösenordshashen för att kunna autentisera användare. Som synes ovan så har vi avaktiverat denna policy på grund av dessa svagheter. Dock så måste en administratör sätta denna policy manuellt på varje användare som vill använda sig av VPN förbindelsen.

Tabell 5, Policy för kontoutelåsning Confidence.local

Inställningar	Användare
Kontoutelåsningens varaktighet	15 minuter
Tröskelvärde för kontoutelåsningen	5 felaktiga inloggnings försök
Återställ räknare för kontoutelåsning efter	15 minuter

Denna funktion används för att låsa konton som skriver in ett visst antal felaktiga lösenord på rad. Denna funktion förhindrar brute force attacker eller liknande när en hacker använder ett program för att pröva sig fram till rätt lösenord.

Kontoutelåsningens varaktighet: I det läge ett konto är låst på grund av felaktiga inloggningsförsök anger den här policyn den tid det skall ta innan kontot låses upp igen

Tröskelvärde för kontoutlåsning: Anger hur många försök en användare får skriva fel lösenord innan kontot låses. Ett lågt värde här minskar risken för att gissnings attacker skall lyckas.

Återställ räknare för kontoutelåsning efter: Värdet som anges på denna funktion är antalet minuter det går innan räknare för misslyckade inloggningsförsök nollställs.

4.8 Säkerhetspolicies på användardatorer

De ovanstående reglerna är de som vi vill ska gälla för alla användare och datorer i domänet. Det finns flera säkerhetsinställningar att göra för att göra sin AD miljö säkrare. Dessa inställningar bör dock placeras på OU:s eftersom att vissa konton behöver mer frihet än andra. För att skapa en säker miljö är det viktigt att ge användare så lite rättigheter till systemet som möjligt för att de skall kunna sköta sina arbetsuppgifter. Eftersom projekt tiden var begränsad hade vi inte tid att sätta oss från scratch och sätta upp alla policies, då det finns hundratals. För att skapa en säker miljö använde vi oss istället av mallar som

rekommenderas av Microsoft för att se till att datorer i nätverket är konfigurerade på ett säkert sätt. Dessa mallar samt dokumentation kan hittas på [30].

Vi använde oss av en mall som var rekommenderad för att säkra Windows XP SP2 datorer som hette EC.Desktop.inf. Denna mall sätter säkerhetspolicies åt oss till datorerna. Vi har testkört dessa policies och de fungerar utmärkt i vår miljö. Tanken är att denna mall skall fungera som en utgångspunkt för användare i miljön och i den mån man behöver ge access till funktioner för särskilda användare kan detta redigeras manuellt i respektive grupps OU.

4.9 Användning av Folder Redirect och Offline files

Ett sätt att uppnå säkerhet i VPN är som skrivet tidigare i denna avhandlig (se avsnitt 3.5) att spara så lite filer som möjligt lokalt på datorn. För att uppnå så hög säkerhet som möjligt har vi rekommenderat att datorerna som ansluter skall vara domänanslutna. Detta är inte en förutsättning för att vår lösning skall fungera men en stark rekommendation för att ha någon form av kontroll av vilka som ansluter till företaget. Domänanslutna datorer ger oss även möjlighet att uppnå central lagring dels genom att mappa upp nätverksenheter via ett login-skript som körs vid inloggning, detta kan givetvis också göras manuellt via en icke domänansluten dator men kan då kräva inställningsändringar av användaren och är inte särskilt skalbart.

Användarna har inte alltid tillgång till Internet för att arbeta vilket gör att de måste spara sina filer lokalt på datorn. I vissa fall kanske inloggningen mot AD måste ske i offline-läge vilket också det förhindrar login-skriptet att mappa upp en nätverksmapp. Detta går att kringgå med hjälp av grupp policyn folder redirect (se 2.11.2). Vi har aktiverat denna grupp policy på alla användare i vår domän vilket innebär att såväl användare lokalt på kontoret som VPN användare kommer att ha denna funktion. Vi har ställt in det så att alla filer på användarnas skrivbord och filerna i mina dokument sparas centralt på en server.

Folder redirect används ofta med offline files vilket ger möjlighet till användaren att komma åt och redigera sina filer utan att vara ansluten till företaget. Fördelarna med att använda folder redirect med offline files är att filerna bara sparas lokalt så länge användaren inte är ansluten till företagets nät. Så fort användaren ansluter till företaget kommer filerna att synkroniseras per automatik utan att användaren behöver göra någonting. Detta hjälper användarna till central lagring och kommer också att hjälpa i de fall inloggnings-skriptet som mappar nätverksdiskar inte går att köra.

Källa: [33].

4.10 Övriga grupp policies av vikt

Förutom de policies som beskrivits ovan finns det en del andra policies av vikt, både i det lokala nätverket men i synnerhet för VPN-anvädning. Nedan beskrivs dessa kortfattat.

Synkronisering av offline filer: Med denna policy kan man styra när offline filer skall försöka synkronisera mot vår server. Vi vill synkronisera filerna när användarna loggar in och loggar av och sätter därför dessa policies. Inställningarna för detta kan hittas genom att gå in i berörd policy och navigera på följande sätt:

User Configuration → Administrative Templates → Network → Offline Files. De berörda policyna som vi slår på är **Synchronize all offline files when logging on** och **Synchronize all offline files before logging out.**

Lösenordsskyddad skärmsläckare: Både i avseende till lokal användning och för VPN-användare är det viktigt att en dator har en lösenordsskyddad skärmsläckare som går ingång efter en viss tid. Detta för att inte utomstående skall kunna komma åt information när slarviga användare lämnat datorn för att gå på kafferast eller helt enkelt glömt att stänga av datorn. För att kontrollera detta finns ett antal policies. För att ställa in dessa navigerar man på följande sätt: **User Configuration → Administrative Templates → Display.** Här hittar vi tre inställningar för att tvinga användarna att använda skärmsläckare.

Screen Saver : Enabeld

Password protect the screensaver: Enabeld

Screen saver Timeout: Enabeld

I den sista policyn får vi sätta ett värde på hur länge användarna skall vara inaktiva innan skärmsläckaren går igång. Denna satte vi till 900 sekunder, det vill säga 15 minuter.

Brandvägg med korrekta inställningar: Denna policy har vi inte använt oss av då vi inte riktigt vet vilka brandväggsinställningar som krävs för de olika applikationer som finns på företaget. Vi tycker dock att det är viktigt att nämna denna då man kan tvinga användarna att använda Windows inbyggda brandvägg och man kan också ställa in vilka program eller portar som skall vara tillåtna. Eftersom vi fokuserat på VPN i första hand så är detta en viktig policy för att se till att klientens brandvägg används och är konfigurerad på korrekt sätt. Inställningarna för brandväggen hittas på följande plats:

Computer Configuration → Administrative Templates → Network → Network Connections → Windows firewall → Domain Profile.

4.11 Policy för VPN användare

VPN innebär att man öppnar sitt interna nätverk för kommunikation med användarna. Detta innebär att man måste ta itu med en del säkerhetsrisker. Vår lösning på Confidence är ganska flexibel eftersom man kan ge användarna tillgång till VPN på olika sätt. Antingen kan man tvinga användaren att ansluta via domänansluta datorer konfigurerade med brandvägg och antivirus och övriga säkerhetspolicies, som beskrivits i tidigare delar i rapporten, som gäller på företaget. Man kan distribuera ett paket som sätter upp alla inställningar som krävs i VPN-programvaran så att användaren är lyckligt ovetande om pre-shared keys som används osv. Denna lösningen är den säkraste och kräver minst av användaren. Det går även om man vill att ansluta datorer till företagets VPN utan att de skall vara domänanslutna från vilken dator som helst. Vid detta läge introduceras en rad säkerhetsproblem eftersom att företagets administratör inte längre har kontroll över maskinen. Problem med denna lösning är till exempel att användaren själv måste se till att tillhandha uppdaterat virusskydd och installerad och konfigurerad brandvägg för att inte utsätta det interna nätverket för risk. Det finns också andra problem med denna lösning som att användaren sparar företagskritisk information till en dator som man inte har någon kontroll över vilka som kan komma åt. Om man av någon anledning måste använda lösningen med hemdatorer som ansluter så finns det en del riktlinjer att ge användaren.

- Var försiktig med företagets matrial
- Låt inte andra inklusive familjemedlemmar använda din jobbdator
- Lämna aldrig din dator utan tillsyn eller olåst
- Använd brandvägg samt ett uppdaterat antivirus program

Utbildning av VPN-användare är givetvis också viktigt framför allt i de fall man tillåter hemdatorer att ansluta. Vilket antivirusprogram bör användas, vilka portar kan vara öppna i brandväggen, vilka inställningar skall användas i VPN programvaran. I de fall användaren får tillgång till företagets pre-shared key som används vid konfigureringen måste användaren bli informerad om hur den skall hanteras och varnad för exempelvis ”social engineering”.

Det finns givetvis en del riktlinjer som gäller för de som har bärbara domänanslutna arbetsdatorer också. Till exempel så måste man se till att användaren direkt meddelar företagets administratör om datorn skulle bli stulen, det gäller naturligtvis hemdatorer också. Den mest grundläggande policyn för VPN-användare är ändå att informera användaren att den säkerhetspolicy som gäller på det interna nätverket också gäller för datorer som ansluter till företaget via VPN. I bilaga 5 sida Bilaga E - finns ett förslag till policy som Confidence skulle kunna använda sig av, den är gjord utifrån en mall som finnes vid [31].

4.12 Problem

Största problemet för oss i detta arbete var att konfigurera och felsöka enheten som skulle fungera som företages ändpunkt för VPN-kommunikation. Eftersom att vi inte hade någon budget så blev det ganska självklart för oss att använda företagets befintliga brandvägg som hade VPN-funktionalitet. Denna enhet var en Huawei Eudemon 100 och såg på förhand ut att möta de krav vi hade på lösningen vi skulle implementera. Nackdelen med denna enhet som vi ganska snart blev varse om var att den enda hjälpen vi hade för att konfigurera den på ett korrekt sätt var en manual, [32]. Eftersom brandväggen främst används på den asiatiska markanden gav den vanliga problemlösaren www.google.com ingen som helst hjälp för oss. Företaget som vi jobbade på saknade också ett supportavtal med brandväggstillverkaren vilket i många fall gjorde det jobbigt eftersom vi inte kunde få feedback på vad vi hade konfigurerat fel. Det var ett problem i den mening att det var tidskrävande. Efter några försök fick vi dock VPN-kommunikationen att fungera, men ett problem kvarstod. Vi lyckades inte få datorer bakom NAT-enheter att ansluta. Som beskrivet i avsnitt 2.10 krävs en funktion kallad NAT-T för att tillåta datorer bakom NAT att ansluta. Enligt manualen skulle enheten stödja denna funktion men vi fick det inte att fungera och eftersom vi inte kunde få tag i någon support stod vi i detta läge helt stilla. Vårt företag lyckades så småningom hjälpa oss i supportfrågan men svaret tog tid och det visade sig att vår brandvägg inte hade support för funktionen. Hade vi vetat detta tidigare hade vi med största sannolikhet rekommenderat företaget att lägga ut lite medel på en annan lösning eftersom detta är en rejäl begränsning.

5 Analys

I denna analys tänkte vi visa vad som händer då en klient kopplar upp sig mot vår VPN-gateway. Vi använder alltså L2TP/IPSec eller L2TP över IPSec för att på ett säkert sätt skapa en tunnel mellan våra klienter och företagets gateway. Det första som sker i anslutningen är att en IPSec SA förhandlas fram. Som tidigare beskrivits används protokollet ISAKMP för att skapa en SA mellan parterna. I Figur 37 illustreras de 9 paket som behövs för att skapa SAs mellan parterna.

Source	Destination	Protocol	Info
192.168.224.60	82.117.[redacted].2	ISAKMP	Identity Protection (Main Mode)
82.117.[redacted].2	192.168.224.60	ISAKMP	Identity Protection (Main Mode)
192.168.224.60	82.117.[redacted].2	ISAKMP	Identity Protection (Main Mode)
82.117.[redacted].2	192.168.224.60	ISAKMP	Identity Protection (Main Mode)
192.168.224.60	82.117.[redacted].2	ISAKMP	Identity Protection (Main Mode)
82.117.[redacted].2	192.168.224.60	ISAKMP	Identity Protection (Main Mode)
192.168.224.60	82.117.[redacted].2	ISAKMP	Quick Mode
82.117.[redacted].2	192.168.224.60	ISAKMP	Quick Mode
192.168.224.60	82.117.[redacted].2	ISAKMP	Quick Mode

Figur 37 Visar upprättandet av en IPSec förbindelse. Dom svarta fälten är Confidence IP-adress vilken vi inte vill lämna ut.

I exemplet ovan vill en klient med IP nummer 192.168.224.60 skapa en anslutning till vår VPN-gateway. När förhandlingen är avslutad har parterna autentiserat varandra, utbytt en hemlig sessionsnyckel samt bestämt vilka algoritmer som skall användas för kryptering samt autentisering. Dessa värden sparas i en databas kallad SAD (Security Association Database). En dator eller en gateway har i många fall flera SAs sparade i databasen och för att identifiera vilken SA som skalla användas till en särskild anslutning används motpartens IP address och ett värde kallat SPI (Security parameter Index). Med hjälp av dessa värden kan vår gateway veta vilken SA den skall använda för att exempelvis kryptera trafik till en särskild dator. I Figur 38 ser vi en aktiv policy i vår VPN gateway

```
connection id: 3224
encapsulation mode: transport
tunnel local : 82.117.[redacted]    tunnel remote: 81.216.[redacted]
flow      source: 82.117.[redacted]/255.255.255.255 17/1701
flow destination: 192.168.1.5/255.255.255.255 17/1701

[inbound ESP SAs]
  spi: 2270998763 (0x875cb0eb)
  proposal: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
  sa remaining key duration (bytes/sec): 255999568/3591
  max received sequence-number: 4
  udp encapsulation used for nat traversal: N
```

Figur 38 Visar hur en aktiv SA ser ut.

När parterna har förhandlat fram SA:n är de redo att säkert utbyta trafik. I Figur 39 ser vi hur trafiken mellan parterna ser ut. Protokollet som används är som synes nedan ESP.

Source	Destination	Protocol	Info
192.168.224.60	82.117.[redacted].2	ESP	ESP (SPI=0x5b742b7d)
82.117.[redacted].2	192.168.224.60	ESP	ESP (SPI=0x3831ef76)
192.168.224.60	82.117.[redacted].2	ESP	ESP (SPI=0x5b742b7d)
192.168.224.60	82.117.[redacted].2	ESP	ESP (SPI=0x5b742b7d)
192.168.224.60	82.117.[redacted].2	ESP	ESP (SPI=0x5b742b7d)
82.117.[redacted].2	192.168.224.60	ESP	ESP (SPI=0x3831ef76)
192.168.224.60	82.117.[redacted]2	ESP	ESP (SPI=0x5b742b7d)

Figur 39 Pågående L2TP/IPSec trafik

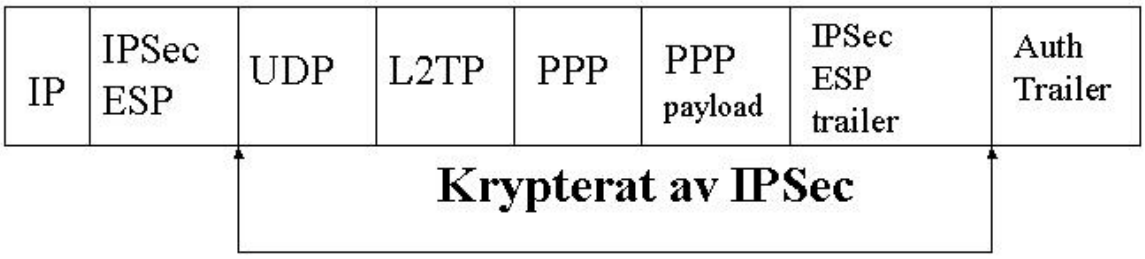
Kollar man närmare på pakten så är de enda värden man kan urskilja SPI. Värdet som alltså används för att identifiera paketet samt sekvensnumret som används för att undvika återspelningsattacker (Figur 40)

```
⊞ Frame 10 (190 bytes on wire, 190 bytes captured)
⊞ Ethernet II, Src: Apple_a0:22:b8 (00:1b:63:a0:22:b8), Dst: Hangzhou_3b:37:30 (00:0f:e2:3b:37:30)
⊞ Internet Protocol, Src: 192.168.224.60 (192.168.224.60), Dst: 82.117.110.2 (82.117.110.2)
⊟ Encapsulating Security Payload
    ESP SPI: 0x5b742b7d
    ESP Sequence: 1
```

```
0020  6e 02 5b 74 2b 7d 00 00  00 01 be 48 41 cf 8b ad   n.[t+}.. ...HA...
0030  a8 06 b9 19 23 b3 4b 84  e6 fb 45 28 e5 a4 0e 05   ....#.K. ..E(....
0040  03 c3 c1 21 41 36 c5 80  5b 4a 85 fe b9 b6 ec e1   ...!A6.. [J......
0050  d3 97 72 4b a0 2c 20 c9  9d 26 96 e6 98 49 dc 78   ..rK., . .&...I.x
0060  66 17 2e 81 80 0a d7 d5  e7 73 29 40 14 12 bb 76   f....... .s)@...v
0070  f6 87 7d 8b d6 13 1d 81  a9 86 9a 2b 03 53 b6 bc   ..}..... ...+.S..
```

Figur 40 Visar ett ESP krypterat paket

När trafiken väl är skyddad av IPSec på detta sätt skapas en L2TP-tunnel mellan parterna. L2TP använder control-paket för att skapa en session i L2TP tunneln över vilken PPP-paket skickas till företagsnätverket. Det som sker är att L2TP kapslar in PPP-paketen som innehåller den ursprungliga data-lasten i ett UDP-paket. All trafik som skickas inklusive användarautentiseringen skyddas då av IPSec. Nedan visas (Figur 41) hur ett paket som skickas över L2TP/IPSec ser ut.



Figur 41 Här ses ett L2TP-paket krypterar av IPSec

6 Slutsatser

6.1 Slutsats

Det mål vi hade när vi började projektet var att skapa en så säker, lätt administrerad och användarvänlig lösning som möjligt. Så här i efterhand tycker vi att vi mött detta mål även om vi inte är helt nöjda med lösningen. Valet av L2TP/IPSec med de starkaste kryptering- och autentiserings algoritmerna som fanns att tillgå får kommunikationen anses som säker. En begränsning finns i autentiseringsmetoden pre-shared key där nyckel distributionen måste ske på ett säkert sätt. För att undvika att nyckeln skickas i mail och via andra osäkra medium skapade vi ett installationspaket, vilket innebär att användarna inte behöver känna till vår Pre-shared-key. Tyvärr så betyder detta inte att lösningen är helt säker då detta paket också kan hamna i orätta händer. En PKI-lösning med certifikat skulle vara mer lättadministrerad och säkrare då man inte skulle behöva oroa sig för distributionen av nycklar. Tyvärr kunde vi inte använda denna lösning då vår brandvägg inte stödde certifikat och vi hade inte heller tillgång till någon maskin att köra en PKI på. I de fall någon skulle få tillgång till vårt paket finns det ett till lager av säkerhet då en användare även måste ha tillgång till ett korrekt användarnamn och lösenord för att få ansluta. Genom användning av RADIUS kunde vi använda samma inloggningsuppgifter i vårt VPN som i resten av företaget vilket både bidrar till att användarna slipper hålla reda på flera användarnamn och lösenord samt drar ner den administrativa delen rejält eftersom en administratör slipper konfigurera användarnamn och lösenord på flera ställen.

Genom grupp policies kan vi centralt sätta upp regler för datorerna som ansluter. Detta innefattar bland annat lösenordspolicy, kontoutelåsning, central lagring av filer, brandväggsintsällningar samt vilka rättigheter användaren har på sin dator. Största problemet med lösningen som diskuterats tidigare är att klienter bakom NAT-enheter inte kan ansluta. Detta är en nackdel då det bidrar till att användarna inte alltid kommer att ha tillgång till vår lösning. Vi har testat ett 3G abonnemang som ger tillgång till publika adresser. Detta fungerar och skulle kunna vara en lösning på problemet.

Det vi har lärt oss är givetvis mycket om olika VPN-lösningar men framför allt har det varit en värdefull erfarenhet att jobba ute på ett företag. Det var en hel del nytt för oss som tidigare mest arbetat i skolmiljöer. Vi arbetade med system och enheter som samtidigt användes av företagets anställda för att sköta sina arbetsuppgifter. Detta gjorde att det krävdes mycket noggrannare planering och undersökning av eventuella fel som kunde uppstå innan implementation. I skolmiljön har vi ofta använt oss av så kallad ”trial and error” teknik där man testar olika inställningar tills man får det att fungera. Denna metod var inte lämplig att använda i företagets miljö där fel konfigureringar kunde innebära att de anställda på företaget inte kunde sköta sina arbetsuppgifter.

En annan lärdom har varit att arbeta bredare med flera olika alternativa lösningar. I skolan har vi många gånger varit bortskämda med att få fördefinierade laborationer som det alltid har funnits en lösning till. I arbetslivet är dock inte problem förbereda av laborationsledare, vilket innebär att alla problem inte har en lösning. Därför bör man arbeta med alternativa lösningar i fall man tvingas förkasta en.

Alla problem vi har haft med lösningen har givetvis inte heller bara varit negativa. Felsökningen och problemlösningen har varit lärorik, vilket har gett oss en ökad förståelse för ämnet.

Om vi skulle göra ett liknande arbete igen finns det en del som vi skulle göra annorlunda. Rapporten är en av de tyngre delarna i ett projekt som detta, där hamnade vi efter redan från början. Det vi skulle ha gjort var att ta reda på hur rapporten skulle se ut och arbeta fram ett skal som passade in i vårt projekt. Sedan komma överens om vad som skulle skrivas, var och hur vi skulle dela upp det oss emellan. En annan sak som vi kunde gjort bättre i början var att läsa på noggrannare om vad Confidence hårdvara klarade av.

6.2 Framtida arbete

Eftersom att denna lösning är långt i från ”perfekt” så finns det givetvis en rad förbättringar som kan göras. Vi känner att vi fått ut det bästa av den lösning vi implementerat, men med lite resurser skulle man kunna göra lösningen avsevärt mycket bättre. De största problemen med nuvarande lösning är NAT-problemet samt användningen av pre-shared key. Med en VPN gateway/server som stödjer certifikat och NAT-T så skulle lösningen både bli säkrare, lättare att administrera samt mer användarvänlig. Vi tror och hoppas att vi byggt en bra grund för framtida förbättringar av detta system med våra lösningar för autentisering och säkerhet. Under projektets gång har vi sneglat på andra lösningar medan vi jobbat med den vi implementerade. Den bästa lösningen med hänsyn till pris tror vi skulle vara att använda Openswan[x] som är en implementation av Linux för VPN. Openswan stödjer både NAT-T och certifikat och skall vara kompatibel med både Windows L2TP/IPSec klient samt MAC OS motsvarighet. Givetvis skulle en Windows server fungera alldeles utmärkt eftersom alla andra produkter vi använder oss av är från Microsoft, det är dock förenat med ytterliggare kostnader. En tredje och sista intressant lösning som man bör undersöka noggrannare om man tar för sig att förbättra den nuvarande lösningen är SSL VPN. Vi har testat OpenVPN som både har stöd för certifikat, radius och fungerar genom NAT utan problem. Det finns också SSL VPN lösningar som gör att vi kommer ifrån klient-delen hos användaren där en SSL stöd webbläsare istället kan användas.

7 Källförteckning

7.1 Referenser

[1] Hamzeh, K. et al. (1999) *RFC 2637 Point-to-Point Tunneling Protocol (PPTP).* IETF Tillgänglig 2007-12-04 på http://tools.ietf.org/html/rfc2637

[2] Mircosoft *Understanding PPTP*. Mircosoft Technet. Tillgänglig 2007-12-04 på http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx?mfr=true

[3] Pall, G & Zorn, G (2001) *Microsoft Point-To-Point Encryption (MPPE) Protocol.* IETF Tillgänglig 2007-12-05 på http://tools.ietf.org/html/rfc3078

[4] Atkinson , R (1995) *RFC 1827 IP Encapsulating Security Payload (ESP).* IETF. Tillgänglig 2007-12-04 på http://tools.ietf.org/html/rfc1827

[5] Maughan, D. et al. (1998) *RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP).* IETF. Tillgänglig 2007-12-04 på http://tools.ietf.org/html/rfc2408

[6] Harkins, D. & Carrel, D. (1998*) RFC 2409 The Internet Key Exchange (IKE). IETF.* Tillgänglig 2007-12-04 på http://tools.ietf.org/html/rfc2409

[7] Bollapragada, V., Khalid, M. & Wainner, S. (2005) *IPSec VPN Design*. Cisco Press. ISBN 1-58705-111-7.

[8] Cisco. CCSP Cisco Secure Virtual Private Networks. Cisco Networking Academy

[9] Malmgren, R., Jonsson, A. (2007) *Nätverkssäkerhet - Teori och praktik.* Tillgänglig 2007-12-04 på http://www.isk.kth.se/kursinfo/6b3008/files/KTH-netsec-2007.pdf

[10] The TCP/IP Guide IP. *Security (IPSec) Protocols. Tillgänglig* 2007-11-25 på http://www.tcpipguide.com/free/t_IPSecurityIPSecProtocols.htm

[11] (2007) *Layer 2 Tunneling Protocol.* English Wikipedia Tillgänglig 2007-12-10 på http://en.wikipedia.org/wiki/L2TP

[12] Townsley, W. et al (1999) *RFC 2662 Layer Two Tunneling Protocol "L2TP"* IETF. Tillgänglig 2007-12-10 på http://tools.ietf.org/html/rfc2661

[13] Microsoft (2007) *Basic L2TP/IPSec Troubleshooting in Windows XP*. Microsoft Technet. Tillgänglig 2007-12-10 på http://support.microsoft.com/kb/314831

[14] Patel, B. et al (2001) *RFC 3193 Securing L2TP using IPSec* IETF. Tillgänglig 2007-12-10 på http://tools.ietf.org/html/rfc3193

[15] Simpson, W. (1994) *RFC 1661 The Point-to-Point Protocol (PPP).* IETF Tillgänglig 2007-12-10 på http://tools.ietf.org/html/rfc1661

[16] Simpson, W. (1994) *RFC 1662 PPP in HDLC-like Framing.* IETF Tillgänglig 2007-12-10 på http://tools.ietf.org/html/rfc1662

[17] Cisco Systems. (2006) *Point-to-Point Protocol.* Cisco Documentation Tillgänglig 2007-12-10 på http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ppp.htm

[18] (2007) *Challeng-handshake authentication protocol.* English Wikipedia Tillgänglig 2007-12-10 på http://en.wikipedia.org/wiki/Challenge-handshake_authentication_protocol

[19] Simpson, W. (1996) *RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP).* IETF Tillgänglig 2007-12-10 på http://tools.ietf.org/html/rfc1994

[20] *Data Encryption Standard(DES)* (1999) National Institute of Standards and Technology(NIST) Tillgänglig 2007-12-04 på http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[21] Broman, P. & Liljerum, O. (2001) *En jämförelse av krypteringsalgoritmer.* Blekinge Tekniska Högskola Tillgänglig 2007-12-04 på http://www.ide.hk-r.se/~nesse/kandidat_200106/Peter_Broman_Ola_Liljerum.pdf

[22] Fredriksson, M., Malmgren, R. & Schlyter (2006) *Introduktion till kryptografi* Tillgänglig 2007-12-04 på http://www.sweden.gov.se/content/1/c6/09/00/70/24b96f76.pdf

[23] Eastlake, D. & Jones, P. (2001) *RFC 3174 US Secure Hash Algorithm 1 (SHA1).* IETF Tillgänglig 2007-12-04 på http://tools.ietf.org/html/rfc3174

[24] Rigney, C. et al (2000) *RFC 2865 Remote Authentication Dial In User Service (RADIUS).* IETF Tillgänglig 2007-12-10 på http://tools.ietf.org/html/rfc2865

[25] Kivinen, T. et al (2005) *RFC 3947 Negotiation of NAT-Traversal in the IKE.* IETF Tillgänglig 2007-12-10 på http://tools.ietf.org/html/rfc3947

[26] Shinder, D. (2005) *NAT Traversal (NAT-T) Security Issues.* WindowSecurity.com/articles Tillgänglig 2007-12-10 på http://www.windowsecurity.com/articles/NAT-Traversal-Security.html?printversion

[27] Shinder, T. (2005) *Remote access VPN and a Twist of Dangers of Split Tunneling.* ISAserver.org Tillgänglig 2007-12-19 på http://www.isaserver.org/tutorials/2004fixipsectunnel.html

[28] Schnier, B (1999) *Cryptanalysis of Microsoft's PPTP Authentication Extensions.* www.schneier.com tillgänglig 2007-12-04 på http://www.schneier.com/paper-pptpv2.html

[29] Schnier, B (1998) *Frequently Asked Questions -- Microsoft's PPTP Implementation.* www.schneier.com tillgänglig 2007-12-04 på http://www.schneier.com/pptp-faq.html

[30] Microsoft (2006) *Windows XP Security Guide.* Microsoft Technet. Tillgänglig 2007-12-04 på http//www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx

[31] SANS Institute (2006) *Virtual Private Network (VPN) Policy.* SANS. Tillgänglig 2007-12-06 på http://www.sans.org/resources/policies/Virtual_Private_Network.pdf

[32] Huawei Technologies CO., LTD. (2005) *Quidway Eudemon 100/200 Firewall Operation Manual*

[33] Microsoft Technet (2002) *Best Practices for Folder Redirection in User Data and Settings Management.* Tillgänglig 2007-12-15 på http://technet2.microsoft.com/windowsserver/en/library/f0fe0826-aade-46cc-9323-22657ebb7c511033.mspx?mfr=true.

7.2 Orefererade referenser

Strebe, M. & Perkins, (2002) *Brandväggar 2:a upplagan.* Pagina. ISBN 91-636-0736-0

Maiwald, E. & Sieglein, *W (2002) Datasäkerhet I praktiken. Pagina*. ISBN 91-636-0752-2

Henmi, A. et al (2004) *Firewall policies and VPN Configurations.* Syngress ISBN 1-59749-088-1

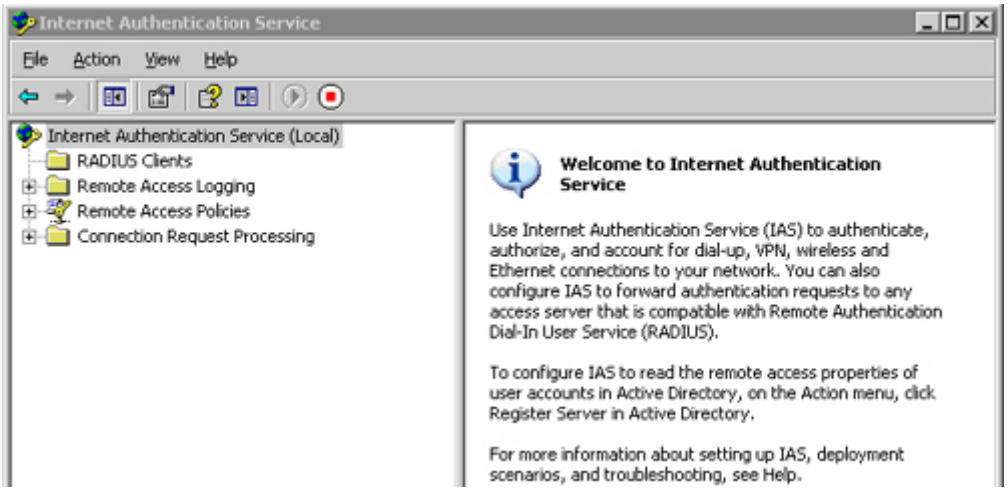
Huawei Technologies CO., LTD. (2005) *Quidway Eudemon 100/200 Firewall Command Reference*

Boswell, W (2003) *Indside Windows Serve.r 2003.* Pearson Education. ISBN 0-7357-1158-5

Honeycutt, J (2003) *Introduktion till Microsoft Server 2003.* Pagina. ISBN 91-636-0775-1

Bilaga A - Installation av Internet Authentication Service (IAS)

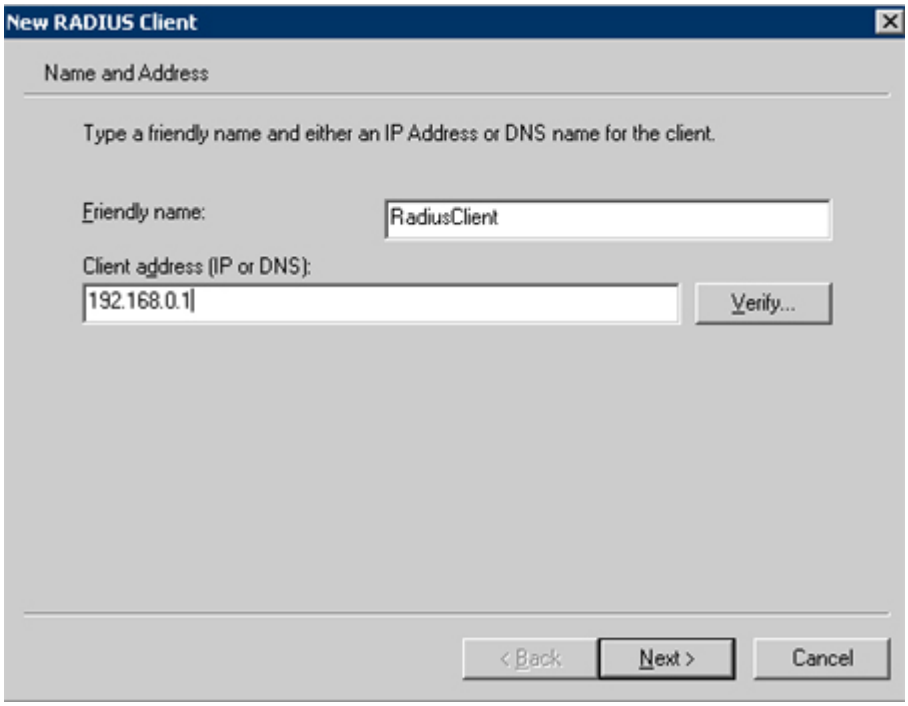
IAS är en radius server gjord av Microsoft som vi använde oss av för användarautentisering och loggning i detta projekt. IAS medföljer i Windows Server 2003 och nedan finns en guide över hur man installerar IAS.



Figur 42 Grundfönstret i IAS.

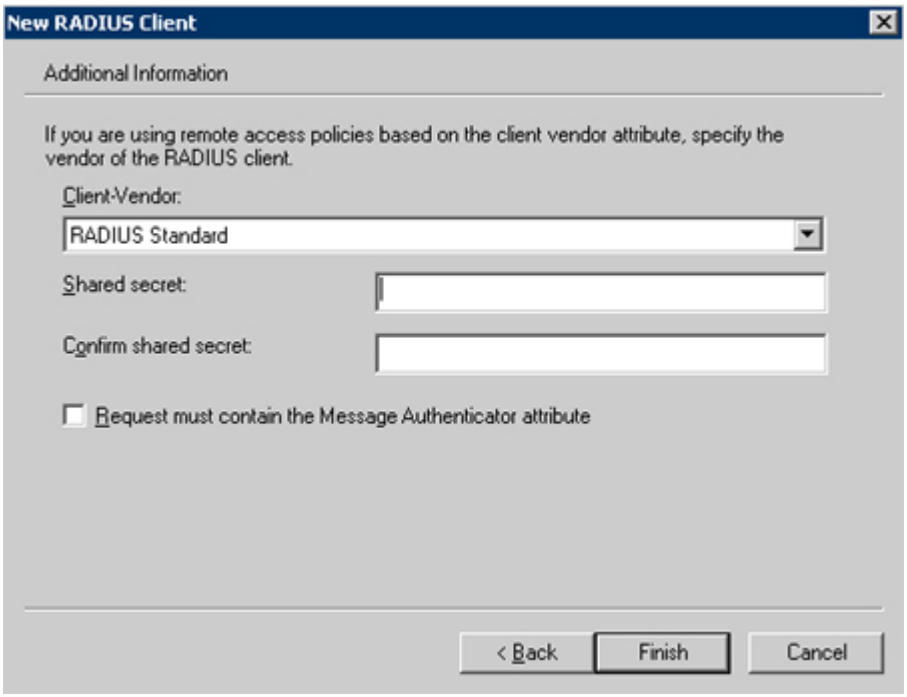
När du öppnar IAS första gången kommer du att se denna ruta. Det första du skall göra nu är att lägga till en RADIUS klient.

-Högerklicka på RADIUS Clients → New RADIUS Client



Figur 43 Skriver in namn och IP på RADIUS klienten.

Välj ett klientnamn och skriv in klientens IP-address. Tryck sedan på Next.



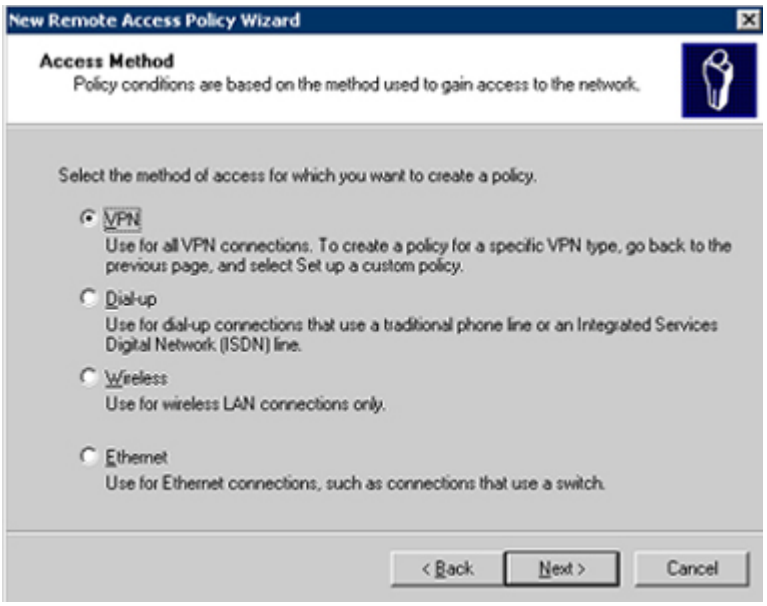
Figur 44 Rutan där man skriver in den delade nyckeln.

Härnäst ska vi bestämma en delad nyckel mellan klienten och servern. När detta är gjort klick på Finish. Vi har nu lagt upp en ny RADIUS-klient.

Efter att RADIUS-klienten är upplagd är det dags att definiera en policy för vilka som ska få tillgång till systemet och under vilka förutsättningar.

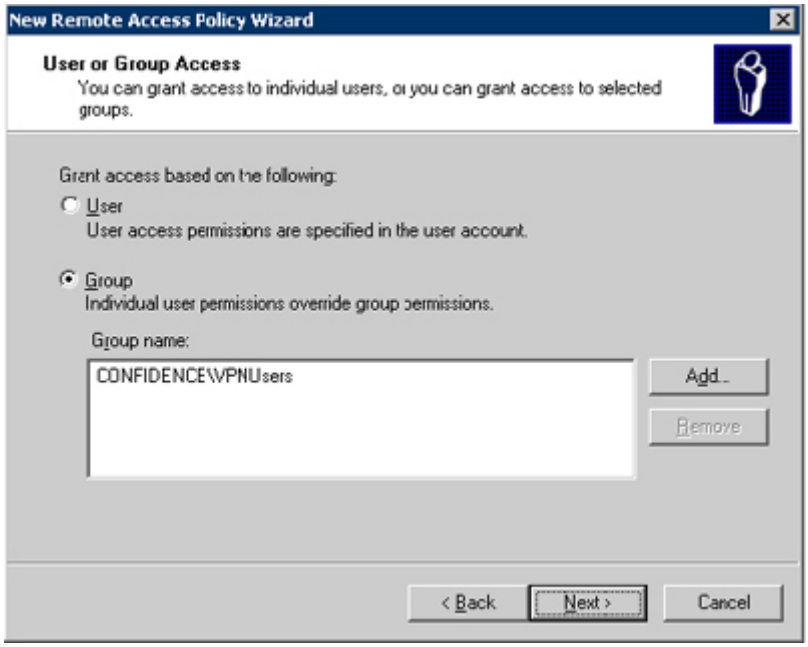
Högerklicka på Remote Access Policies → Create Remote Access Policy

Du får nu upp en guide. Klicka Next vid första rutan. I nästa ruta använder vi oss av en guide för att sätta upp regler för hur vi vill autentisera fjärranvändare. Kryssa i rutan med alternativet Use the wizard to setup a typical policy for a common scenario välj ett namn på din nya policy och klick på Next.



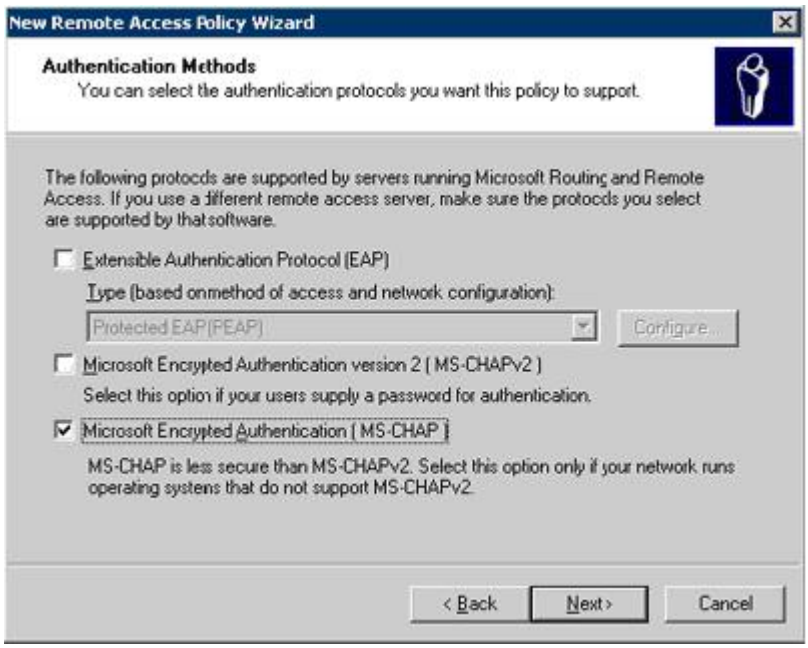
Figur 45 Här väljer man accessmetod för den här policyn.

I detta fall skall vi skapa en policy för VPN-användare. Därför kryssar vi i VPN i denna ruta och trycker på Next.



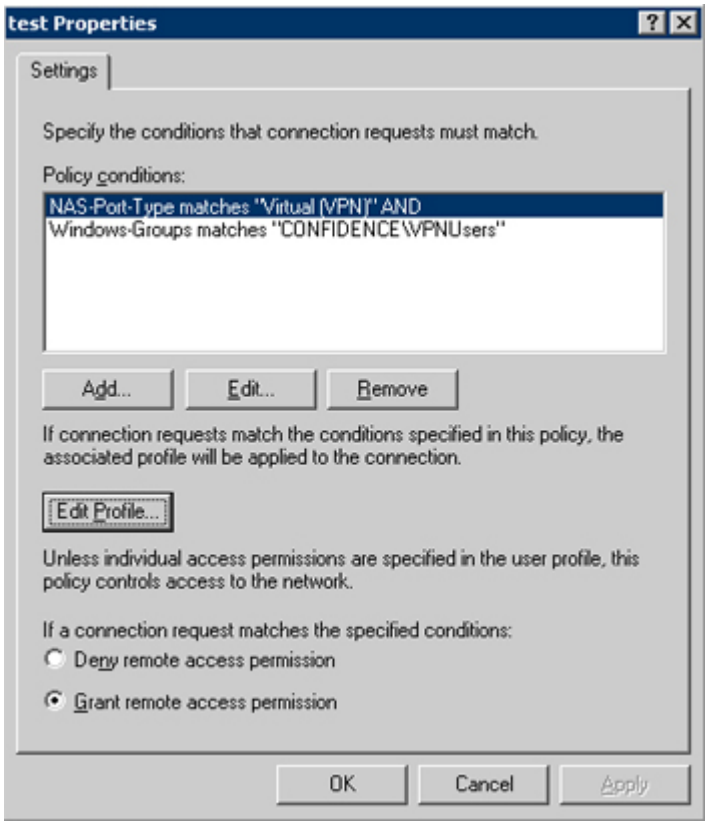
Figur 46 Väljer man vilken policy som skall tillämpas för vår VPN anslutning

Nu är det dags att bestämma vilka som skall får ansluta via VPN till vårat nätverk. Vi ligger till den grupp med användare som vi vill ska ha tillgång till att ringa in och klicka på Next.



Figur 47 Här väljer vi den autentiseringsmetod som skall användas.

I nästa ruta i wizarden ska du välja vilken autentiserings metod som skall användas. I detta fall kommer vi att använda oss av MS-CHAP.



Figur 48 Här ser vi vilka regler som används.

Därefter är vår policy klar. Denna policy kommer att tillåta användare från gruppen VPNUsers att ansluta via VPN med autentiseringsprotokollet CHAP. Om du vill ändra i policyn kan du enkelt högerklicka på den välja properties och sätta andra parametrar.

Meningen är att användarna skall autentisera sig mot AD. För att kunna göra detta måste IAS-servern registreras i AD.

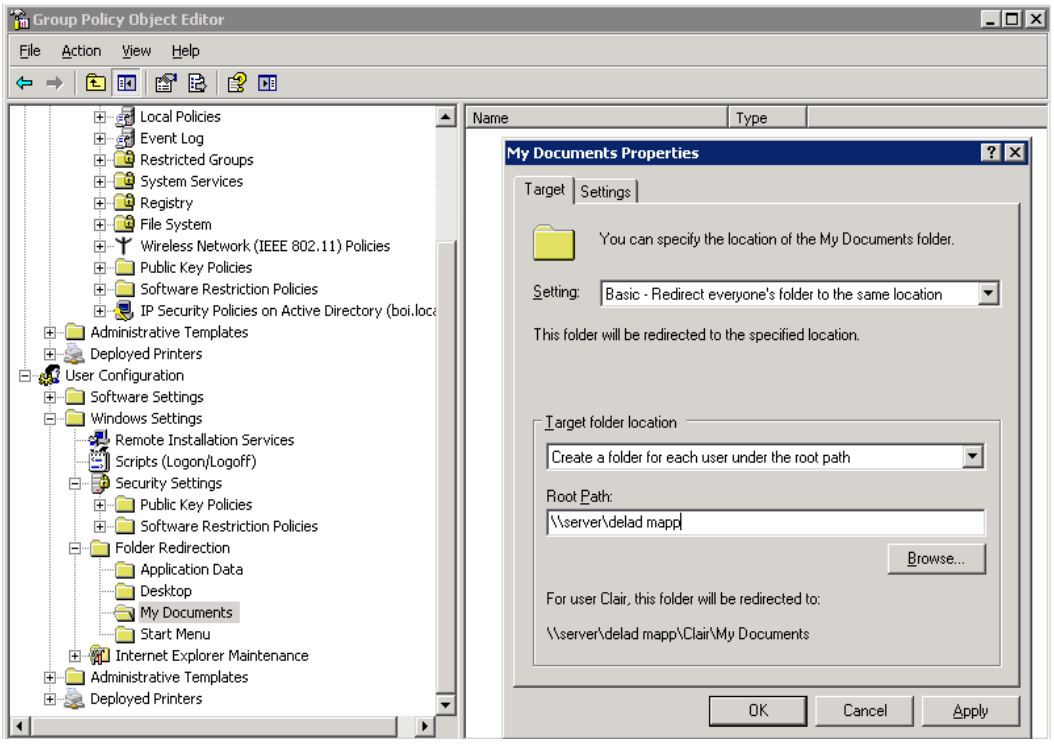
Bilaga B - Konfigurering av Folder redirect och Offline files

Folder Redirect är en grupprincip som sätts på användare. Vi valde att använda denna funktion på alla användare i domänet och ställde därför in denna princip i ett grupprincipobjekt länkat till den OU-behållare som innehåller alla vår användar avdelningar vilken är OU:n Confidence Sweden AB users. Innan vi konfigurerar principen måste vi ha en delad mapp på servern där vi senare skall lagra användarnas mappar. Denna mapp placerade vi på disk på domänkontrollanten på C://Folderredirect

När denna mapp var klar skapad vi ett GPO objekt till OU:n ovan. För att aktivera och konfigurera folder redirection går får man navigera sig till följande del i GPO:n

User Settings --> Windows settings --> Folder Redirection

I detta läge kan man välja vilka delar av användarens profil som skall sparas på servern. För vårt syfte att spara data centralt så valde vi att spara mapparna Mina dokument och skrivbordsmappen. För att ställa in detta högerklickar man på respektive mapp och väljer properties. När det är gjort får man fram följande fönster (Figur 49).



Figur 49 Visar vart man lägger till en sökväg till en delad mapp.

Vi använde inställningarna ovan där vi helt enkelt bara anger UNC (Universal Naming Convention) sökvägen till vår delade mapp som vi skapade tidigare. Efter detta klickar vi bara **ok** och sedan tar Windows automatiskt hand om resten. Windows kommer sedan att ställa in offline-inställningar på mapparna samt skapa mappar åt användarna med korrekta rättigheter under rootmappen. Användarna kommer att stå som ägare till sina mappar och

ingen annan kommer åt dem. Administratörs kontona kan givetvis ta över ägandet av mappen om man så vill.

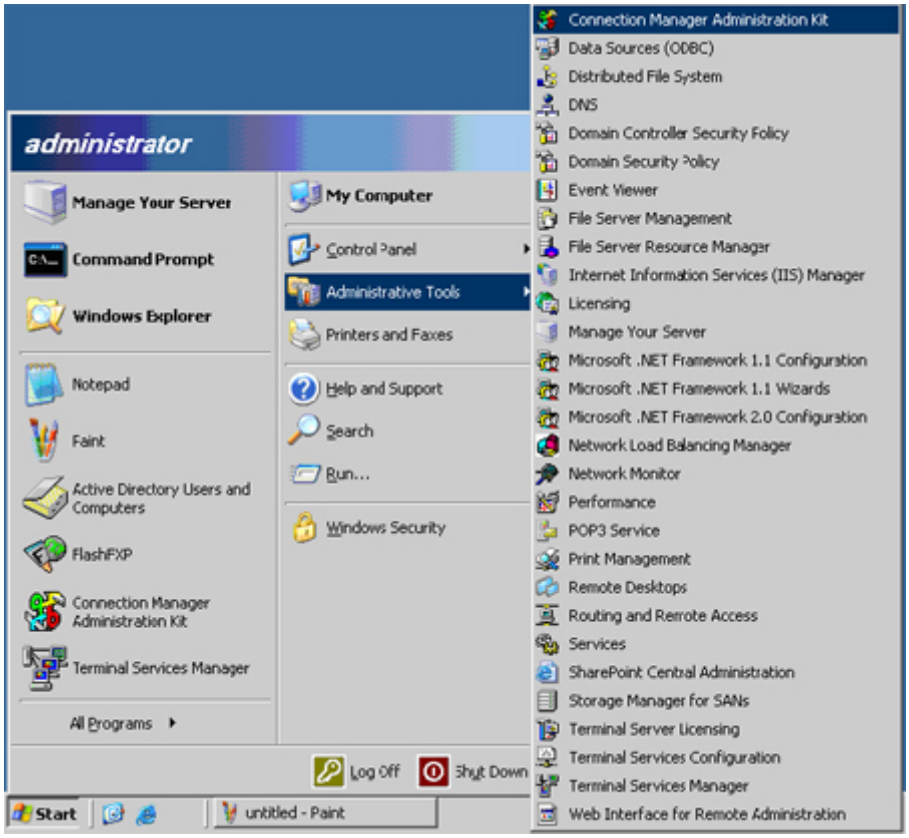
Bilaga C - Bilaga 3 – Konfiguration av CMAK

CMAK (Connection Manager Administration Kit) gör det möjligt att göra installationsfiler till klienter som konfigurerar en VPN anslutning med valda inställningar. Detta ger många fördelar då administratören på företaget både sparar tid eftersom man snabbt kan sätta upp VPN anslutningar på klienter. Det är också möjligt att göra MSI-paket av dessa installationsfiler och distribuera dem via AD. En annan fördel med CMAK är att många inställningar i VPN-klienten blir låsta, vilket bidrar till att man förhindrar användaren att använda ”farliga” säkerhetsinställningar som till exempel Split-tunneling. Man kan också konfigurera eventuell Pre-Shared-key i denna installation vilket också är den fördel.

CMAK ingår i Windows Server 2003 och man installerar det genom att gå in i kontrollpanelen → Add or Remove programs. I Add or Remove programs fönstret klickar vi på **Add/Remove Windows Components** knappen. I fönstret Windows Components wizard välj **Management and monitoring tools** och trycker på **details** knappen. Man kan här välja att installera **Connection Manager Adminstration Kit**.

När CMAK är installerat kan man börja konfigurera VPN-anslutningar. Nedan kommer en guide på hur vi gick till väga för att skapa installationsfiler till våra användare.

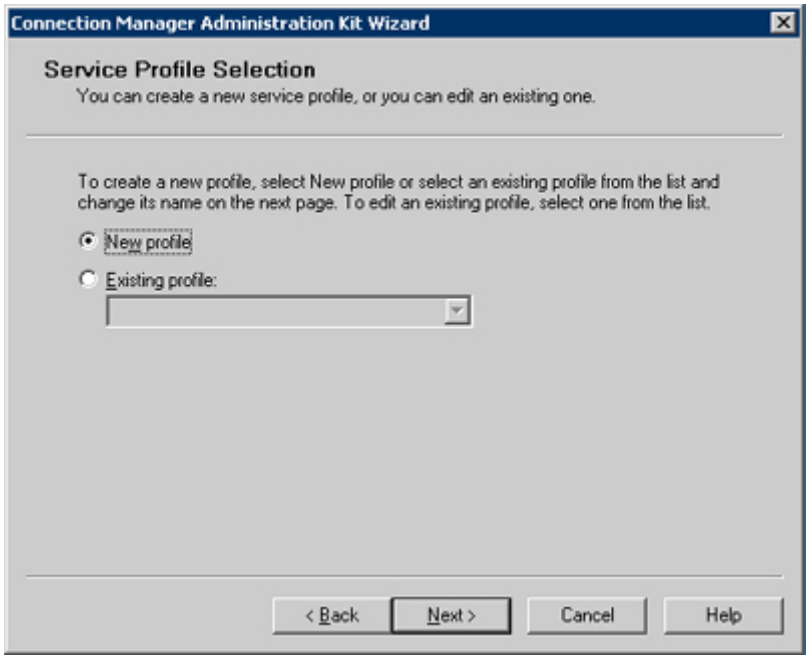
5. Starta CMAK genom att klicka på startmenyn→ Administrative tools → Connection Manager Administration Kit



Figur 50

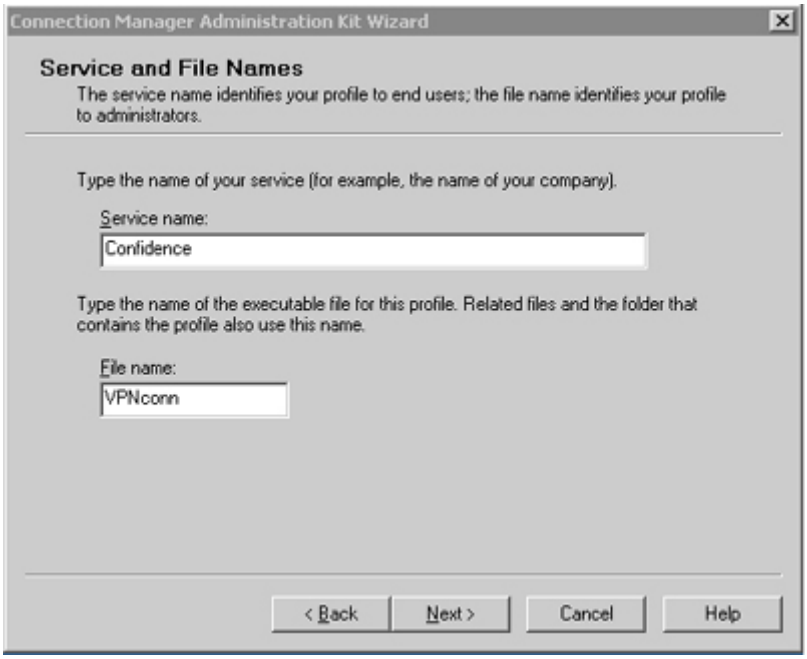
6. Du möts nu av fönstret Welcome to the Connection Manager Administration Kit Wizard. För att starta guiden klicka du på Next.

7. Du kommer nu få välja om du vill skapa en ny profil eller om du vill editera en gammal profil. Eftersom att vi inte har någon tidigare profil väljer vi valet New Profile och klickar på Next.



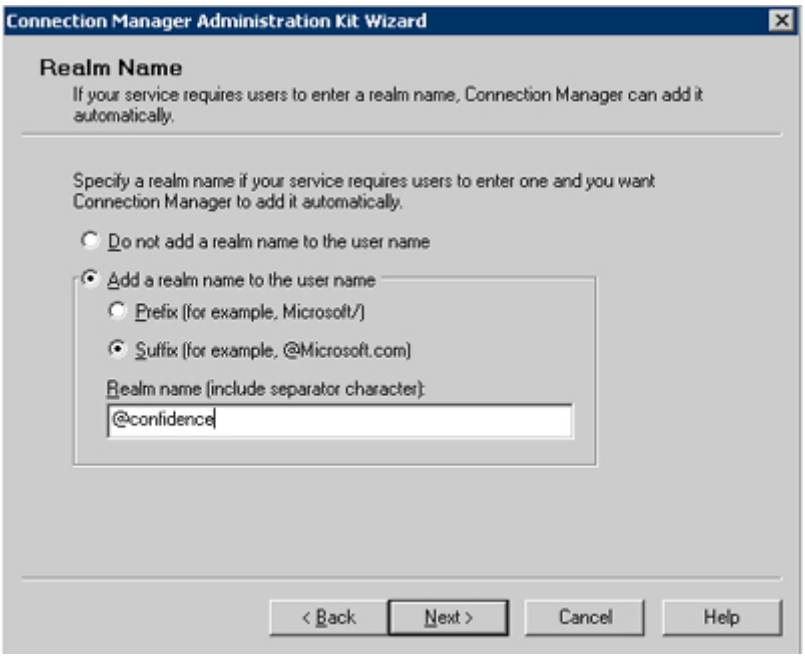
Figur 51

8. Nu måste vi välja ett service namn och ett filnamn. Service namnet kommer att vara det namn som uppkopplingen kommer att få. Medan filnamnet är det namn vår installationsfil kommer få. Vi skriver in något i stil med det vi ser på bilden nedan.



Figur 52

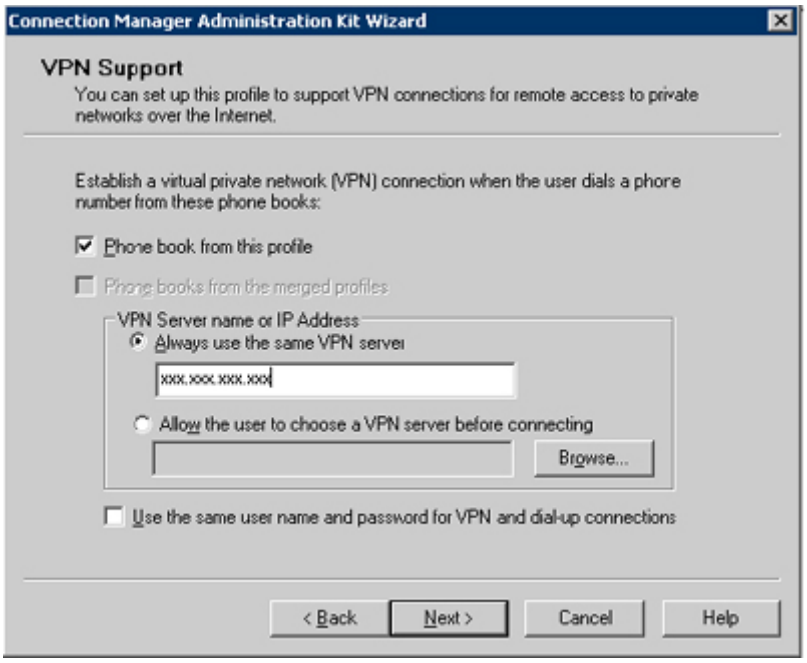
9. Nästa ruta guiden ger oss är Realm Name. Denna ger oss möjlighet att lägga till ett realm till användarens namn. Man behöver inte lägga till ett realm men i vårat fall kommer det att underlätta eftersom att vi använder realmen confidence i vår brandvägg. Det kommer att underlätta för användarna att bara behöva skriva in användarnamnet istället för användarnamn@confidence.



Figur 53

10. Nästa ruta ger oss möjlighet att förena tidigare gjorda inställningar i profiler med den nuvarande. Eftersom vi inte har gjort några profiler tidigare så klickar vi **Next.**

11. Nästa del i guiden är VPN-Support. Här ställer man in adressen till vår VPN-gateway. Här finns det möjlighet att ange flera VPN-gateways och låta användaren välja vilken de skall ansluta sig till. Eftersom vi bara har en VPN-gateway så skriver vi in ip adressen till denna och klickar sedan **Next.**

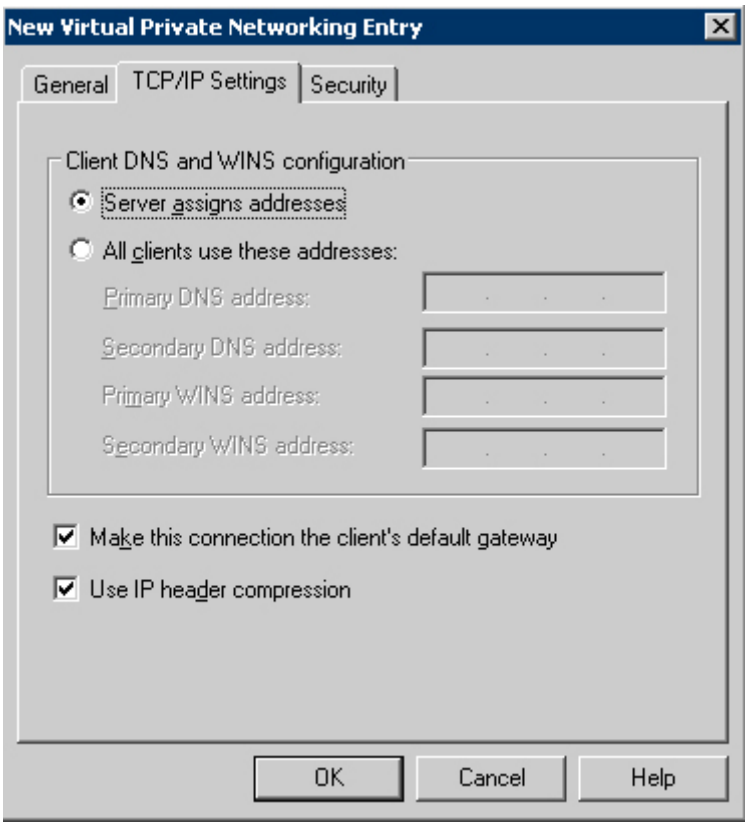


Figur 54

12. Härnäst ska vi konfigurera TCP/IP och andra säkerhetsinställningar för anslutningen. För att göra det måste man klicka på **Company VPN Tunnel (Default)** i listan och trycka på **edit.**

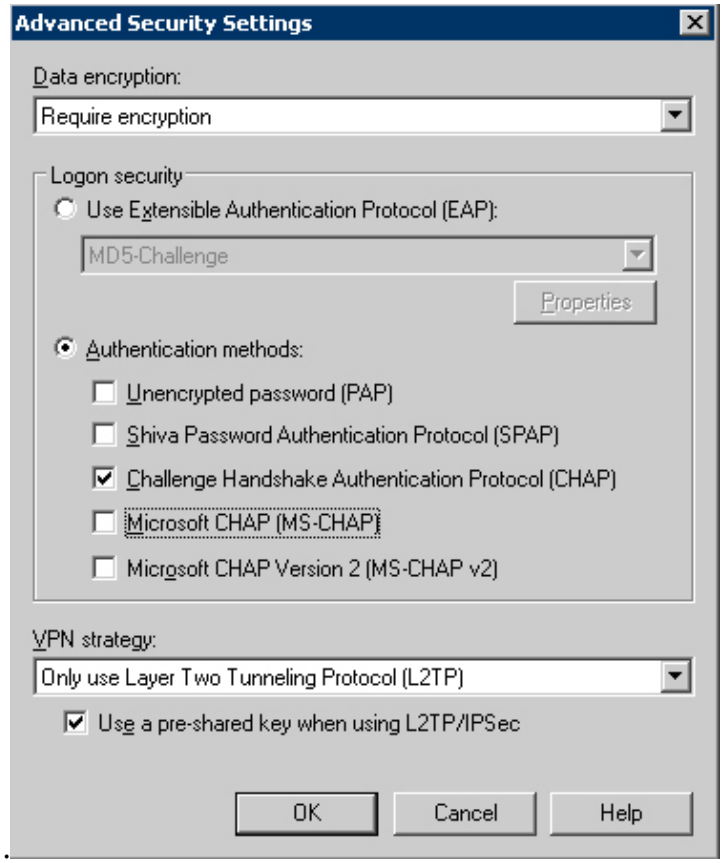
13. I första fliken **General** använder vi default inställningarna, det är ganska självförklarande

14. I andra fliken TCP/IP Settings väljer vi att vår VPN server ska tilldela oss ip-addresser istället för att manuellt ange dem. Vi förhindrar också split tunneling genom att se till att **Make this connection the client's default gateway** alternativet är ikryssat.



Figur 55

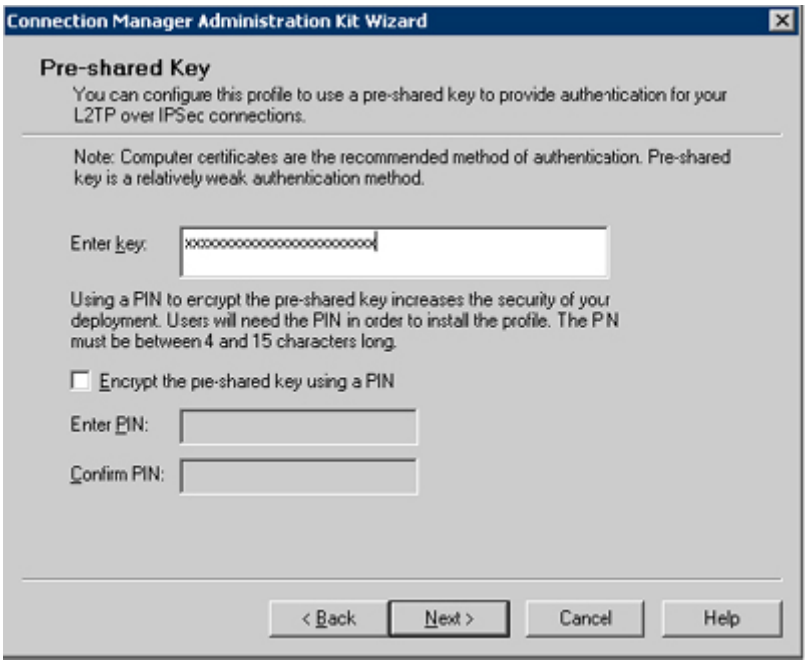
15. I sista fliken **Security** väljer vi först **Use advanced security settings** under security settings. Basic alternativet används om man vill ha stöd till äldre operativsystem. Efter vi markerat advanced alternativet klickar vi på Configure. Vi väljer inställningarna som skall användas för vår anslutning och klickar sedan på **Next.**



Figur 56

16. När detta är inställt klickar man **Ok** och sedan **Next.**

17. Nu är det dags att fylla i den Pre-Shared key som skall användas. Det finns möjlighet att kryptera denna nyckel med en PIN kod men för att göra det enkelt för användarna har vi struntat i detta alternativ.



Figur 57

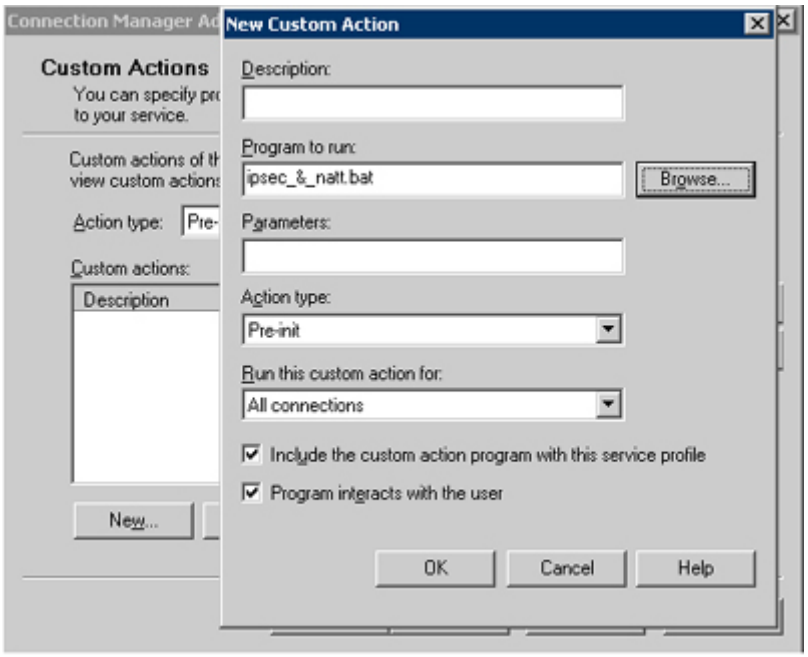
18. Nästa ruta, **Phone Book,** kommer vi inte att använda oss av. Klicka därför ur alternativet **Automatically download phone book updates** och klicka sedan **Next.**

19. Nästa ruta kommer vi heller inte att använda då det gäller uppringda anslutningar. Klicka **Next**

20. Nästa ruta berör oss inte heller då vi inte använder oss av split tunneling. Om man skulle tillåta split tunneling skulle man här kunna skapa nya routes i klientens routing tabell, vilket skulle ge VPN-användaren tillgång till de subnät på det interna nätverket som vi vill. Vi kommer inte att ändra i routing tabellen och klickar därför **Next.**

21. I Automatic Proxy Configuration kan man tvinga VPN-klienten att använda företagets interna brandvägg som dess Web proxy server. Med detta alternativ kan man tvinga användaren att använda företagets brandväggs policy så länge klienten är kopplad till det interna nätverket.

22. I nästa ruta kan man välja att köra program innan, efter eller under olika delar av VPN-uppkopplingen. Eftersom vi enligt tidigare text kräver att vissa skript körs lokalt på datorerna för att vår VPN-koppling skall fungera. Vi väljer att bifoga dessa skript här innan uppkopplingen börjar i pre-init läge. Detta görs genom att klicka på **New** och sedan bläddra sig fram till de program man vill köra via **Browse** knappen. När programmet är tillagt klickar vi på **OK.**

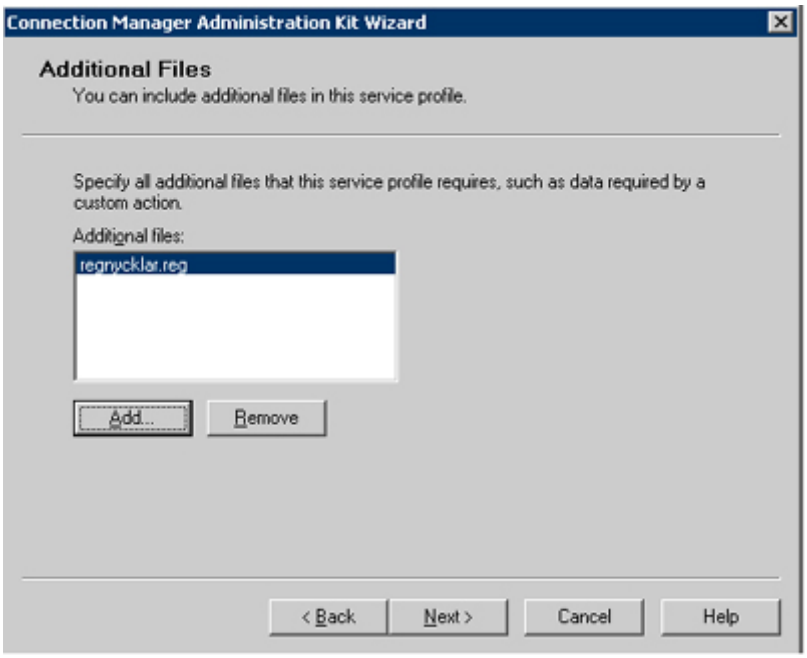


Figur 58

23. Nästkommande steg i guiden ges det möjlighet att ändra de grafiska delarna i VPN-klienten samt lägga till ytterliggare information till användaren. Vi går inte igenom dessa steg här, man kan nämna att man kan lägga till hjälpavsnitt, support telefonnummer, licensavtal samt välja ikoner.

24. Vi klickar fram till fönstret Additional Files. Där man kan lägga till valfria filer som kommer att följa med installationsmappen. Här lägger vi till registernyckel skriptet

som det program som vi lade till i steg 22 använder sig av. Man klickar helt enkelt på **Add** och pekar på filen man vill lägga till. Vi klickar sedan på **Next.**



Figur 59

17. Nu är vi framme vid det sista steget. Vid Ready to build your service profile klickar vi på **Next.** och sedan kommer CMAK att bygga ett installations program med våra konfigureringar åt oss. Dessa kommer att sparas under **C:\Program Files\CMAK\Profiles.**

Bilaga D - Registernyckel Skript

Vår skriptfil innehåller följande rader:

```
CLS
@echo off
TITLE regedit filer
ECHO.
ECHO Applying regedit
REGEDIT /S regnycklar.reg
ECHO.
```

Filen regnycklar.reg som anropas i skriptfilen ovan ser ut såhär:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters]
"ProhibitIpSec"=dword:00000000
;Either it accepts IPSec or denie it. value of 1 denies IPSec
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPsec]
"AssumeUDPEncapsulationContextOnSendRule"=dword:00000002
;Turns on UDP encapsulation for NAT-T to work in IKE negotiation. Value of 2 accepts nat on both sides.
```

Bilaga E - Fjärranslutnings policy

Policy för fjärranslutning

1.0 Syfte

Syftet med denna policy är att ge riktlinjer för fjärranslutning till Confidence företagsnät.

2.0 Omfattning

Denna policy gäller för alla anställda, konsulter, vikarier på Confidence som har tillgång till fjärranslutning till Confidence företagsnät.

3.0 Policy

Godkända användare på Confidence kan få tillgång till fjärransluta till Confidence företagsnät. För att användaren skall kunna utnyttja tjänsten måste hon ha tillgång till en Internet anslutning. I vissa fall krävs det att användaren har tillgång till vissa programvaror för att använda tjänsten. Eventuell kostand för detta står användaren för. För hjälp med att konfigurera och komma igång med tjänsten kontaktas IT-avdelningen på Confidence.

Dessutom gäller följande:

25. Det är användarens ansvar att se till att obehöriga användare inte ges tillgång till Confidence företagsnät

26. När användaren är uppkopplad mot företagsnät kommer av säkerhetsskäl alla trafik till och från datorn att gå via en krypterad tunnel. Detta innebär att användare inte till exempel kommer att kunna surfa på Internet medan man är ansluten till företaget.

27. VPN-tjänsten konfigureras och hanteras av IT-avdelningen på Confidence. Eventuella frågor om tjänsten kan riktas hit.

28. Alla datorer som ansluter till Confidence företagsnät måste ha ett uppdaterat antivirus program installerat.

29. Användare av säkerhetsskäl automatiskt bli frånkopplade från Confidence företagsnät vid inaktivitet i 15 minuter.

30. Ansluta användare kan maximalt vara ansluta till Confidence företagsnät i 8 timmar. Efter detta krävs det att användaren loggar in igen.

31. Datorer som tillåts ansluta till företagsnätet som in ägs av Confidence måste helt lyda de VPN-policies och IT-policies som är framtagna av Confidence

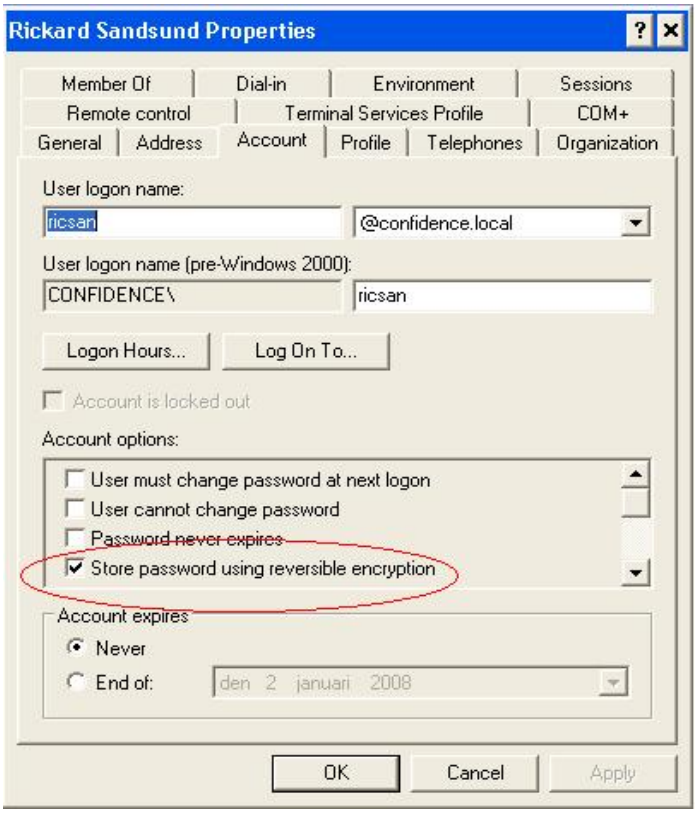
32. När användaren ansluter till företaget med personlig utrustning måste användaren förstå att maskinen faktiskt blir en del av Confidence nätverk och därför måste samma regler gälla för denna som för alla datorer i Confidence nätverk.

4.0 Tillämpning

En anställd som bryter mot denna policy kan dras inför disciplinära åtgärder, vilket kan innebära uppsägning. [5]

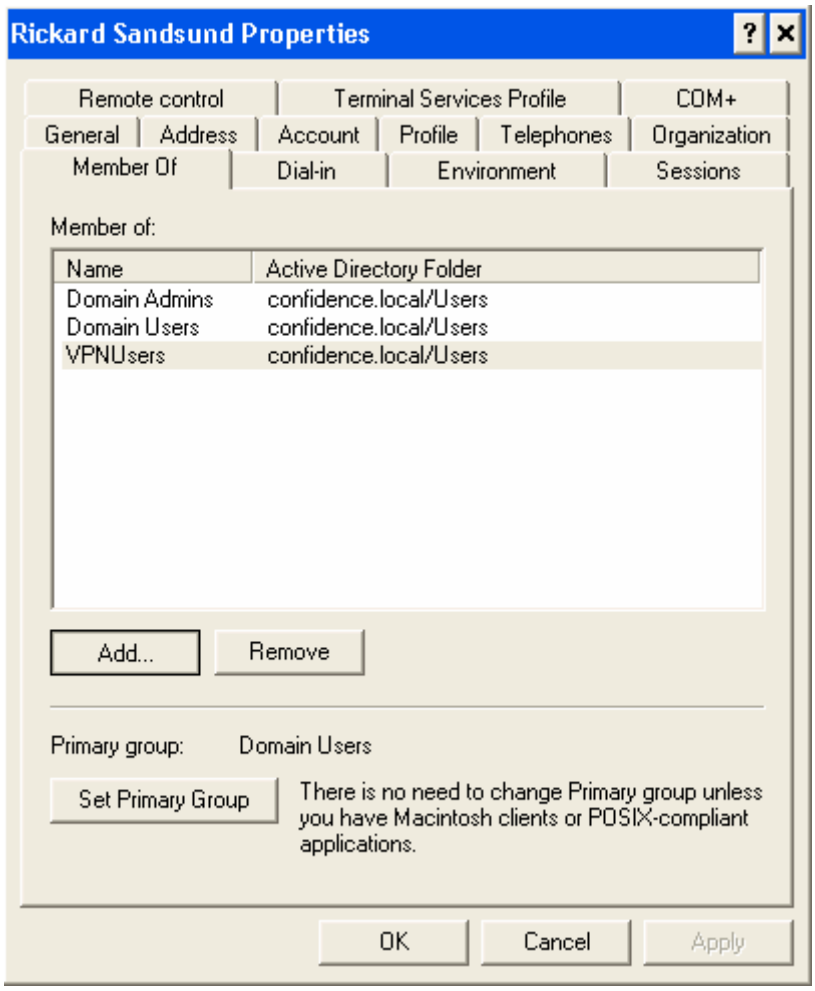
Bilaga F - Inställningar för VPN

Nedan beskrivs det som måste göras för att tillåta en användare att ansluta till företagets VPN. På serversidan måste till att börja med användaren ha ett konto i Active Directory. För att vår autentisering via radius skall fungera måste vi använda oss av omvändbara lösenord. Kryssa för rutan **Store passwords using reversible encryption** för de användare som skall använda VPN (Se Figur 60)



Figur 60 Visar vart i en användares inställningar man väljer hur man ska spara lösenordet.

För att användarna skall kunna ansluta måste de också ingå i den grupp som har rättighet att ansluta via VPN. Denna grupp heter VPNUsers. För att ändra detta går man in på det konto man vill tillåta VPN från och klickar på fliken **Member Of.** Där väljer man **Add** och skriver in VPNUsers (Se Figur 61 nedan)



Figur 61

På klientsidan krävs det också en del konfigurering. För att underlätta detta har vi skapat ett konfigureringspaket (Se Bilaga 3 – Konfiguration av CMAK sid 67). I de fall man vill konfigurera klienten manuellt måste man göra en del inställningar. Till att börja med måste man ändra ett registervärde för att IPSec skall fungera. Följ dessa steg.

33. Klicka på **Kör** i startmenyn.

34. Skriv **regedit,** tryck **ok.**

35. Navigera fram till:
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters

36. Tryck på **New** och välj **Dword Value,** Skriv sedan in **ProhibitIPSec** i textrutan och tryck på Enter.

37. Dubbelklicka på **ProhibitIPSec,** och skriv in **0** i textboxen.

38. Avlsluta genom att trycka på **ok.**

När detta är gjort krävs en omstart av datorn.

När registervärdet är ändrat är det dags att börja konfigurera klienten. Detta kan man göra genom att gå in i **Kontrollpanelen → Nätverksanslutningar → Guiden ny anslutning**

Du kommer nu att gå igenom en wizard som kommer hjälpa oss att konfigurera klienten.

39. Börja med att starta guiden genom att trycka **Nästa.**

40. I typ av nätverksanslutning bockar vi i alternativet **Anslut till nätverket på min arbetsplats.** Tryck sedan **Nästa.**

41. I Nätverksanslutning väljer vi Anslutning till **Virtuellt Privat Nätverk**. Och klickar därefter på **Nästa.**

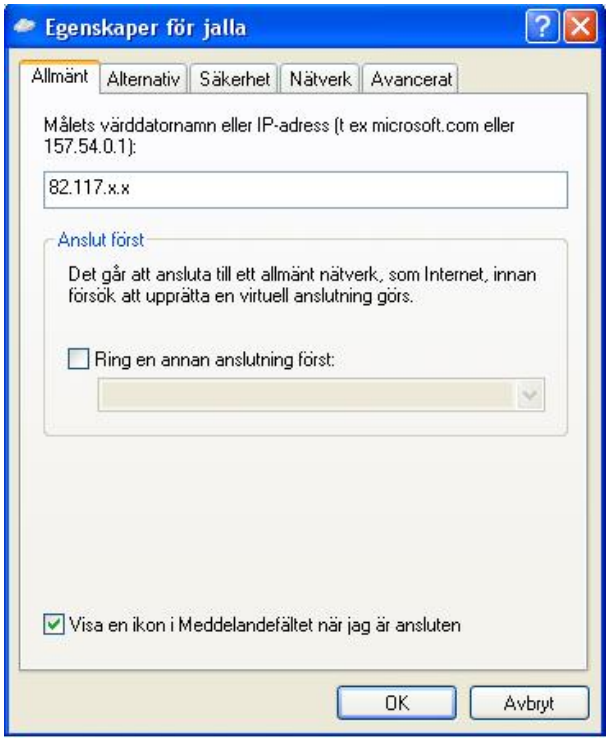
42. I anslutningens namn väljer vi ett passande namn för anslutningen och klickar sedan **Nästa.**

43. I rutan Offentligt nätverk kan man välja att först koppla upp sig på Internet eller till ett annat nätverk innan kopplingen mot vår VPN sker. Vi förutsätter i detta fall att vi redan har en uppkoppling till Internet och väljer därför att bocka för rutan **Ring inte upp en annan anslutning först.** Och sedan **Nästa.**

44. Nu kommer Val av VPN-server. Här skriver vi in vår VPN gateways IP-address och klickar på **Nästa.**

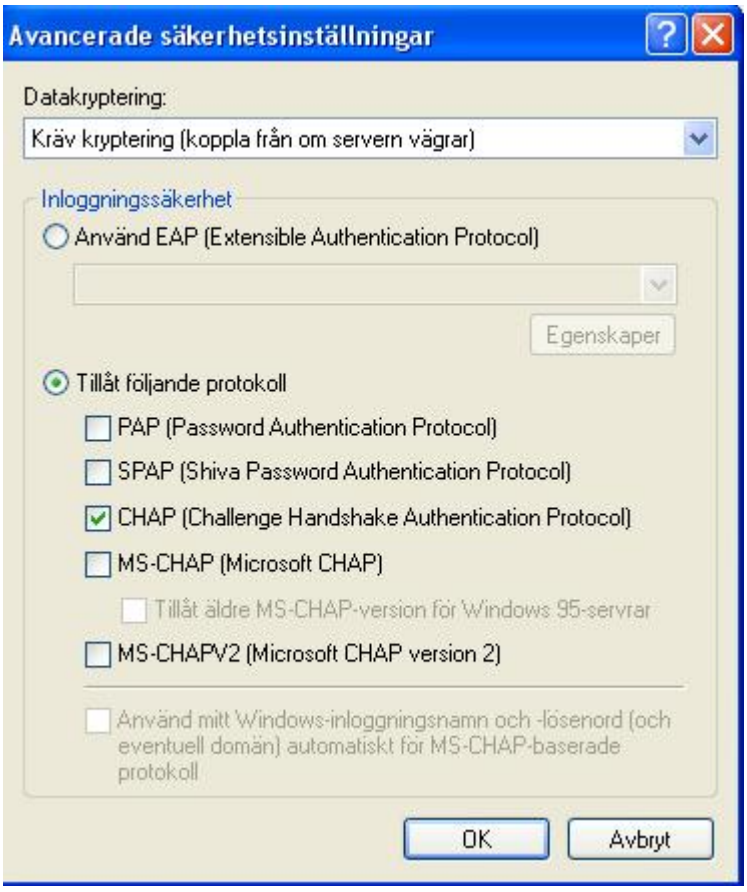
45. Guiden är nu klar och vi avslutar det hela genom att klicka på **Slutför.**

Vi har nu lagt en grund för vår anslutning men vi är inte riktigt klara än. I nätverksanslutningar har det nu skapats en ny nätverksanslutning med det namn vi valde i steg 4. För att göra ytterliggare några inställningar som krävs högerklickar vi på denna och väljer **Egenskaper.** Du kommer nu att mötas av följande fönster (Figur 62 nedan)



Figur 62

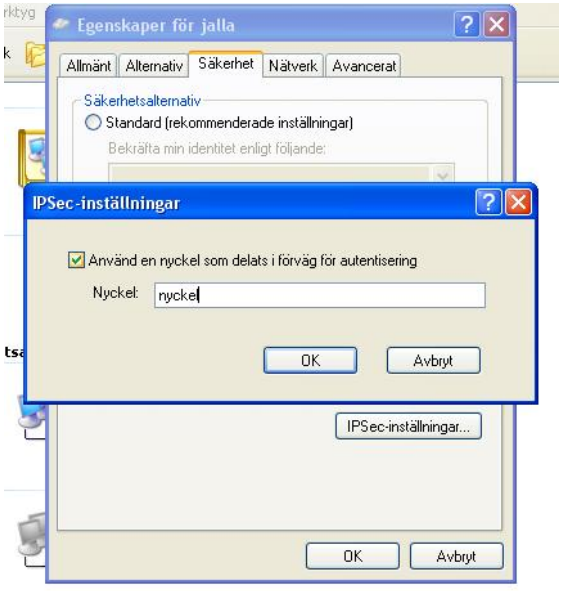
Vi kommer att behöva gå in på fliken **Säkerhet.** Här bockas rutan **Avancerade (anpassade inställningar) i.** Vi möts då av denna ruta (Figur 63) där vi väljer samma alternativ som i bilden nedan.



Figur 63

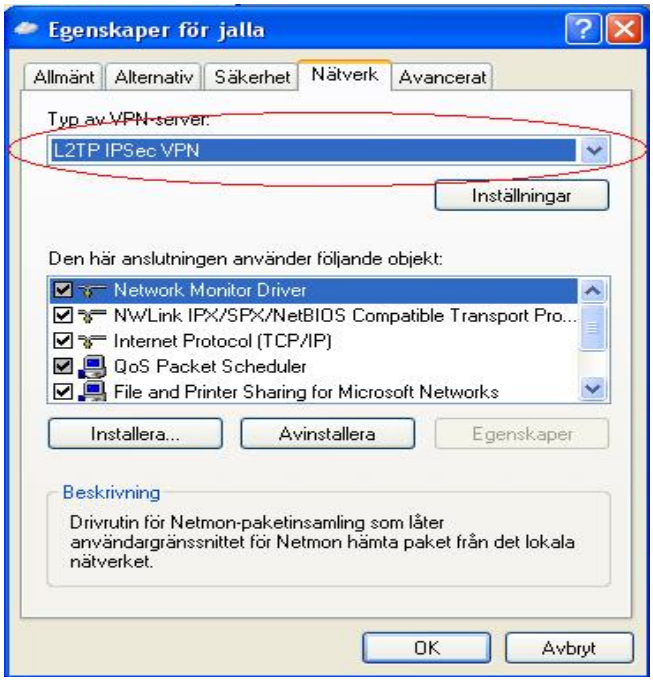
När vi gjort ovanstående inställningar klickar vi på **OK.** När detta är gjort klickar vi på

IPSec-inställningar och får nu skriva in vår fördefinierade nyckel. Enligt Figur 64. När denna är inskriven klickar vi på **OK.**



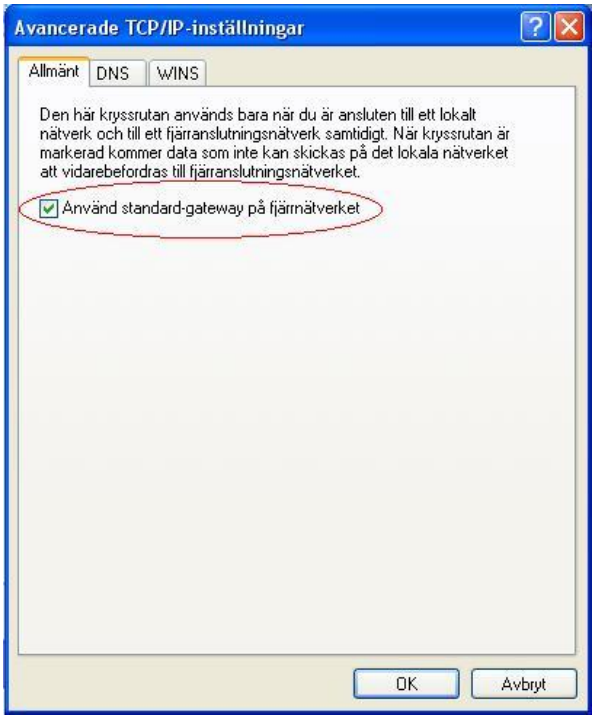
Figur 64

Vi klickar sedan på fliken Nätverk. Här väljer vi **L2TP IPSec VPN** i rullisten **Typ av VPN-server.** Se Figur 65.



Figur 65

När detta är gjort skall vi slutligen markera **Internet Protocol (TCP/IP)** och klicka på **Egenskaper.** En ny ruta kommer nu fram där vi kan specificera IP-inställningar för anslutningen. Dessa ska stå på **Erhåll en IP-adress automatiskt** samt **erhåll adress till DNS-servern automatiskt**. När vi verifierat att detta är fallet klickar vi på **Avancerat** och kan här välja om vi vill tillåta Split tunneling. Rekommendationen är att inte använda detta och vi klickar därför i kryssboxen enligt Figur 66 nedan, klickar på **OK** och sedan **OK** igen. Klienten är nu färdigkonfigurerad.



Figur 66

Det är nu dags att ansluta. Vi dubbelklickar på den ikon vi precis har skapat och får då upp ett fönster som uppmanar användaren att skriva in ett användarnamn och lösenord. De uppgifter som skall matas in här är dem samma som används för inloggning på företagets datorer. Användarna måste dock ange sitt användarnamn följt av domänprefixet @confidence. Till exempel kalle@confidence (Se Figur 67 nedan).

Figur 67

Ett vanligt fel till att anslutningen misslyckas är att IPSec-tjänsten inte är igång. Denna kan kontrolleras genom att högerklicka på **Den här datorn** och där välja **hantera**. I De fönster som nu kommer fram klickar vi oss fram till **tjänster.** Väl där får man leta upp **IPSec-tjänster** bland dom andra tjänsterna och se till att starta den om den av någon anledning inte skulle vara igång. För att göra detta högerklickar man på namnet och väljer **start.**

Bilaga G - De olika Attribute värdena i ett RADIUS paket

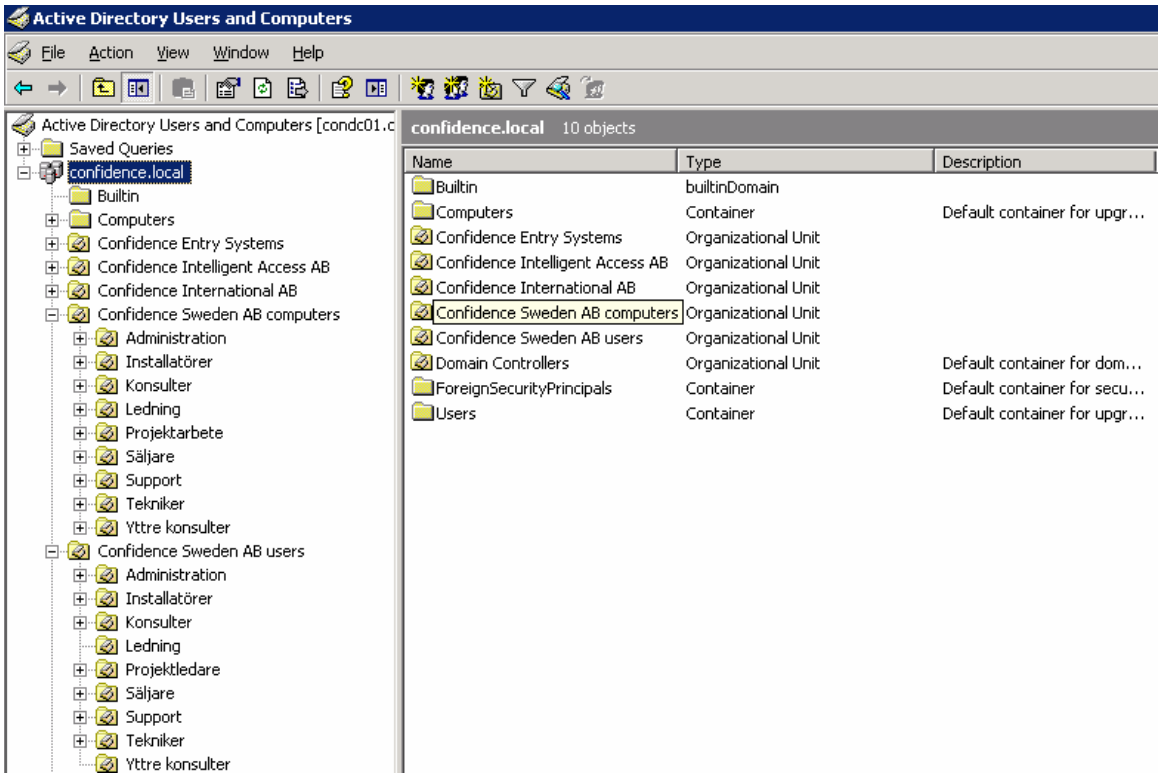
Lista på dom olika typerna som finns, dess kod och längd.

Type	Description	Attribute Length
1	User-Name	=3
2	User-Password	=18
3	CHAP-Password	=19
4	NAS-IP-Address	6
5	NAS-Port	6
6	Service-Type	6
7	Framed-Protocol	6
8	Framed-IP-Address	6
9	Framed-IP-Netmask	6
10	Framed-Routing	6
11	Filter-Id	=3
12	Framed-MTU	6
13	Framed-Compression	6
14	Login-IP-Host	6
15	Login-Service	6
16	Login-Port	6
17	(unassigned)	N/A
18	Reply-Message	=3
19	Login-Callback-Number	=3
20	Framed-Callback-Id	=3
21	(unassigned)	N/A
22	Framed-Route	=3
23	Framed-IPX-Network	6
24	State	=3

25	Class	=3
26	Vendor-Specific	=7
27	Session-Timeout	6
28	Idle-Timeout	6
29	Termination-Action	6
30	Client-Port-DNIS	=3
31	Caller-ID	=3
32	NAS-Identifier	=3
33	Proxy-State	=3
34	Login-LAT-Service	=3
35	Login-LAT-Node	=3
36	Login-LAT-Group	34
37	Framed-AppleTalk-Link	6
38	Framed-AppleTalk-Network	6
39	Framed-AppleTalk-Zone	=3
40	Acct-Status-Type	6
41	Acct-Delay-Time	6
42	Acct-Input-Octets	6
43	Acct-Output-Octets	6
44	Acct-Session-Id	=3
45	Acct-Authentic	6
46	Acct-Session-Time	6
47	Acct-Input-Packets	6
48	Acct-Output-Packets	6
49	(reserved for future accounting)	N/A
192 - 223	(reserved for experimental use)	N/A
224 - 240	(reserved for implemention-specific use)	N/A
241 - 255	(reserved: DO NOT USE)	N/A

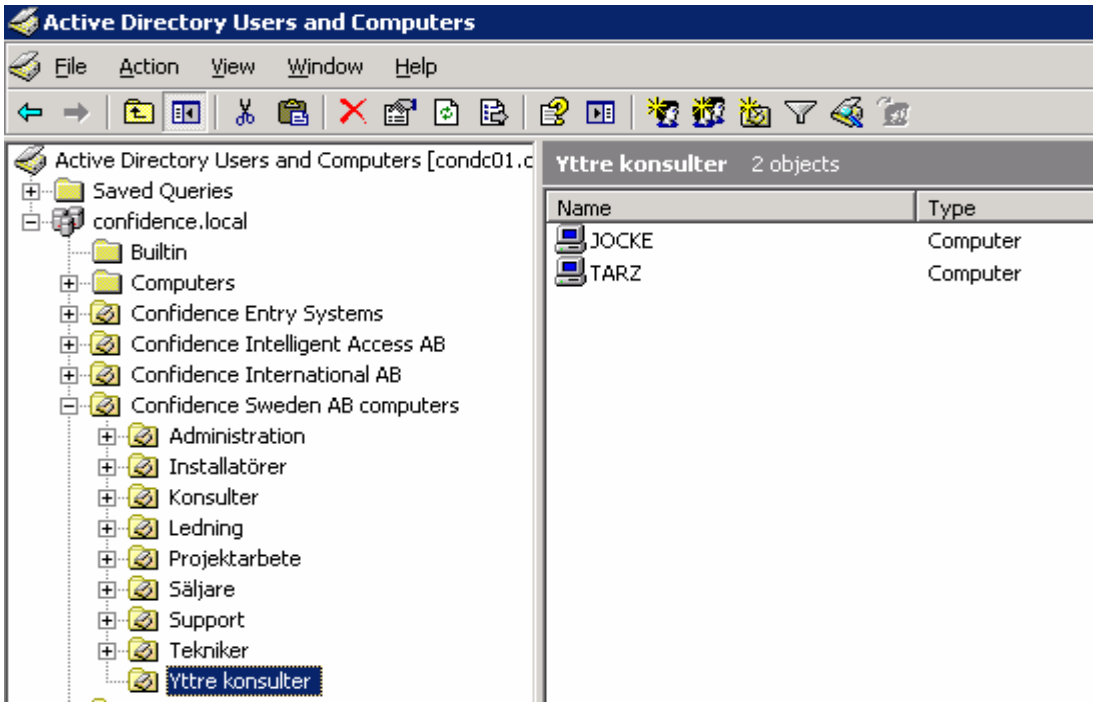
Bilaga H - Guide Grupp policies

Grupp principer eller Group policies är en viktig funktion i Active directory (AD) som erbjuder centraliserad hantering och konfigurering av datorer och användare i ett Active Directory domän. Grupp policy inställningar sparas i så kallade Group Policy Objects (GPO:s) i Active Directory. Dessa GPO:s kan man sedan binda till datorer och användare genom att placera dem i behållare och länka GPO:s till dessa behållare. En behållare kan vara en site, ett domän eller en Organizational Unit (OU). Man placerar helt enkelt användare som man vill ska ha samma policies i en behållare och länkar en GPO till denna behållare. Givetvis krävs den en hel del kunskap om hur AD är uppbyggt för att göra detta på ett korrekt sätt. För att göra det här med grupp policies lite klarare, för er som inte använt det förut, följer ett litet exempel på hur man kan göra för att underlätta administrationen med hjälp av grupp policies. Nedan kan man se en ganska typisk struktur i ett företag även om det finns flera sätt att strukturera detta på beroende på hur ens organisation ser ut.



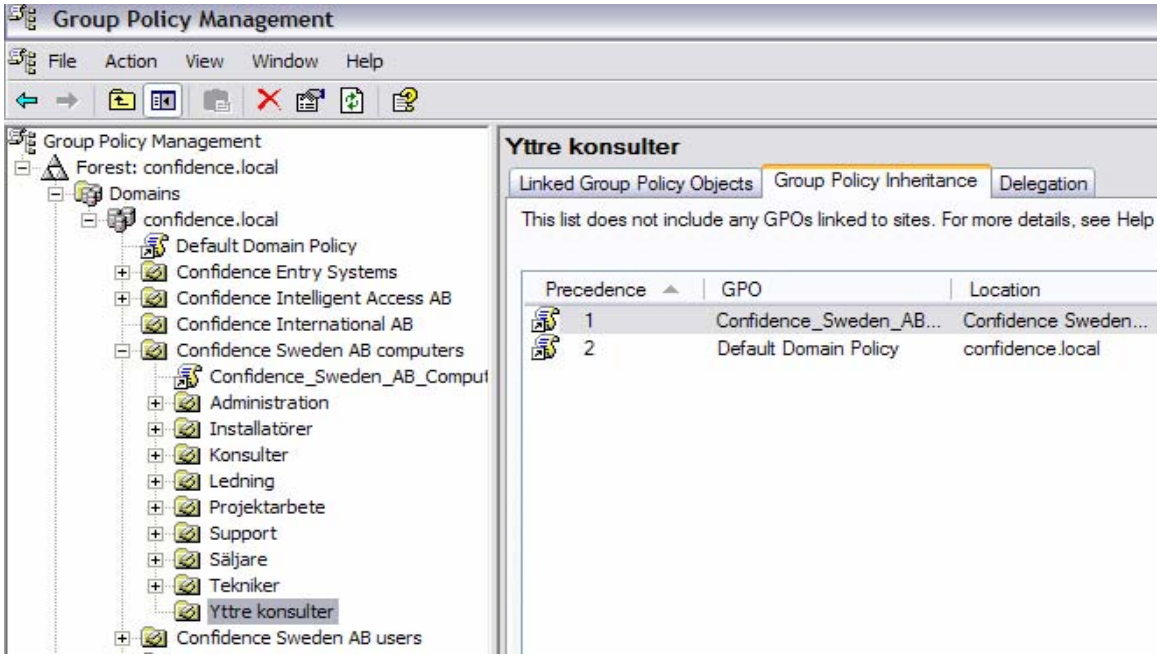
Figur 68

I exemplet ovan har man delat upp organisationen i olika behållare. I dessa behållare kan man sätta olika objekt som man vill ska ha samma policies. Exempelvis ser man på bilden nedan att i OUn Yttre konsulter finns två datorer placerade.



Figur 69

Om vi nu vill applicera en policy på dessa datorer behöver vi bara länka en GPO till OU:n yttre konsulter. På bilden nedan kan vi se att vi i detta här exmpel inte lagt en policy på Yttre Konsulter än. Däremot har vi lagt en policy både på OU:n Confidence Sweden AB Computers och på domänet Confidence.local. Dessa policies kommer att ärvas nedåt då alla principer i ett OU också gäller för dess så kallade child OU:s.



Figur 70

Om vi i det här läget skulle vilja sätta en grupp princip på dessa datorer, exempelvis öka säkerheten, distribuera programvara eller öppna en port i brandväggen kan vi enkelt göra detta genom en policy på denna specifika OU. Möjligheterna är stora då det finns en mängd policies att använda sig av både för domänets användare och datorer.

Ovanstående var ett enkelt exempel för ni som inte använt er av grupp principer i AD tidigare. Det finns massor av fördefinierade policies som man kan använda sig av och vi kommer inte ta upp dessa vidare i denna uppsats.

8 Sakregister

U

V,W

COS/CCS 2007-30

www.kth.se