Groepspaper netwerken

28 januari 2006

Inhoudsopgave

1 Inleiding

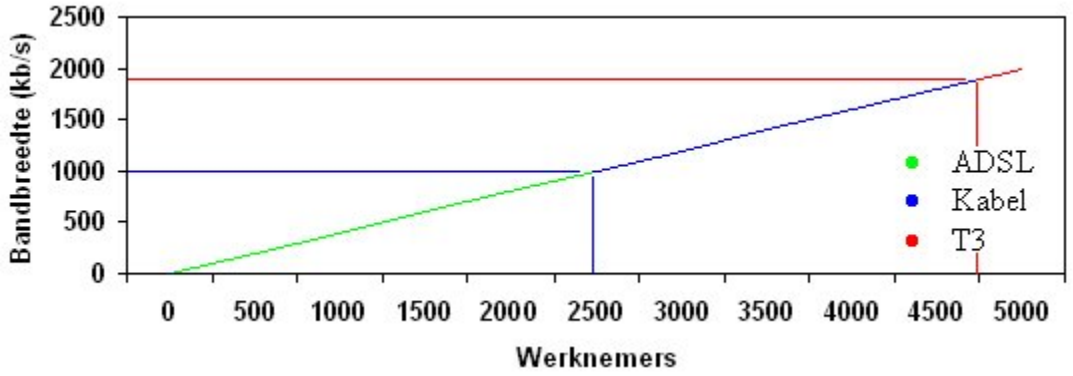
In dit paper bespreken we in redelijk detail de automatisering van een multinational ontstaan uit overnames en fusies met bedrijven uit verschillende landen. De multinational heeft een hoofdkantoor in een (elektronisch ontwikkeld) land, en meerdere kantoren in andere, mogelijk onderontwikkelde landen.
De onderneming wil alle communicatie elektronisch laten verlopen, en niet langer alleen via de telefoon en fax. Ook wil het de verschillende administraties en netwerken van al zijn kantoren integreren.
In dit schrijven hebben we geprobeerd een zon volledig mogelijk aanbeveling te geven naar aanleiding van de te gebruiken structuren, architectuur, protocollen, en internetaansluitingen. Ook wordt er ingegaan over de kosten die het met zich meebrengt, de beveiliging van het elektronische verkeer en de algemene betrouwbaarheid van het aanbevolen systeem.
Dit werk is geschreven in het kader van het informaticavak Netwerken, gegeven in 2005/2006 door drs. P. van Oostrum aan de Universiteit Utrecht.

Met vriendelijke groet,
Wesley, Geerten, Stefan, Pieter, Chris, Jacob, Albert-Jan, en Gerben.

2 Lijnen

De oplossing voor onze multinational qua lijnen, bestaat niet uit 1 lijn. Als dit kon was het makkelijk geweest. We namen overal een T3 lijn en we hadden de beste verbinding momenteel mogelijk. Maar deze lijn is nog niet overal (standaard). Je zou erover kunnen denken om het aan te leggen, maar dit wordt weer erg duur. Om te kiezen wat voor verbinding gekozen wordt en voor waar moeten de voor- en nadelen dus zorgvuldig tegen elkaar opgewogen worden.

Er zijn verschillende mogelijkheden. Het beste is dus T3. Deze lijn zou je moeten huren wat erg duur is. Voordeel is dat het erg snel gaat (45 Mb/s) en betrouwbaar is. Ideaal dus voor e-mail, intensief internet-gebruik, netwerken en natuurlijk Voice over IP.
Aangezien dit erg duur is zal dit worden gebruikt voor het hoofdkantoor en diverse belangrijke kantoren. Een stapje terug is de T1. Dit blijft duur, maar is wel goedkoper. Snelheid is 1.54 Mb/s.
Ook een mogelijkheid is om de lijn (T1 of T3) te delen met een ander bedrijf. Dit scheelt in de kosten. T1 zal worden gebruikt waar nog geen T3 is, maar het wel profitabel is om zon dure lijn te leggen.
Voor kantoren met minder mensen en/of minder belangrijke taken zal ADSL of internet via de kabel (coaxiale kabel) gekozen worden. Snelheid ligt hiervan nog redelijk hoog , namelijk 512 kb/s tot 24 Mb/s voor ADSL/ADSL2 en 10 Mb/s tot 20 Mb/s voor de kabel).
ADSL en kabel kan ook nog aangelegd worden. Nog een stap lager heb je ISDN of internet via de telefoonlijn. ISDN valt nog te gebruiken voor e-mail en licht internetgebruik (snelheid is 56 tot 200 kb/s), maar zal in praktijk niet of nauwelijks gebruikt worden.
Een andere optie, voornamelijk voor landen met slechte infrastructuur, is internet via de satelliet. Deze techniek is zo ver gevorderd dat het te gebruiken is voor thuis en voor bedrijven. Het werkt door middel van een Two Way verbinding, waarmee je een een download en een upload kanaal hebt. Snelheden van 700 kb/s tot 2 Mb/s zijn te halen. VPN kan ook gebruikt worden via satelliet. Deze verbinding zal gebruikt worden voor ontwikkelingslanden, waar enige mogelijk tot communiceren een (slechte) telefoonlijn is.



Deze grafiek laat zien de benodigde verbinding bij een aantal werknemers voor VoIP. Ervan uit wordt gegaan dat gemiddeld 20 procent van de werknemers en gemiddeld 20 kb/s bandbreedte nodig is voor VoIP. Dit geld alleen voor landen die hier gebruik van kunnen maken. Ontwikkelingslanden hebben namelijk sowieso satelliet nodig.
T3 zal dus weinig gebruikt worden vanwege de hoge kosten, maar noodzakelijk bij erg grote kantoren. Kabel zal het meeste gebruikt worden, vanwege goede snelheid en relatief lage kosten en daarna ADSL of ADSL2.

2.1 Kosten

De kosten van de benodigde schotel voor internet via de satelliet en installatie daarvan zijn afhankelijk van het type schotel (74 cm tot 180 cm) dat geplaatst moet worden en varieert van ongeveer 800 euro tot ongeveer

3000 euro. Deze eenmalige kosten moeten natuurlijk betaald worden voor elke vestiging van het bedrijf in een ontwikkelingsland dat we op deze manier willen aansluiten op internet.
Verder moeten er maandelijkse abonnementskosten betaald worden. Dit bedrag is afhankelijk van het aantal gebruikers in onze vestiging. Kleine bedrijven, met tot 5 werknemers op het internet kosten ongeveer 150-250 euro per maand, voor 10 aansluitingen zullen de kosten ongeveer 500-600 euro zijn en voor nog grotere bedrijven (20) moeten we rekenen op een bedrag van duizend euro.

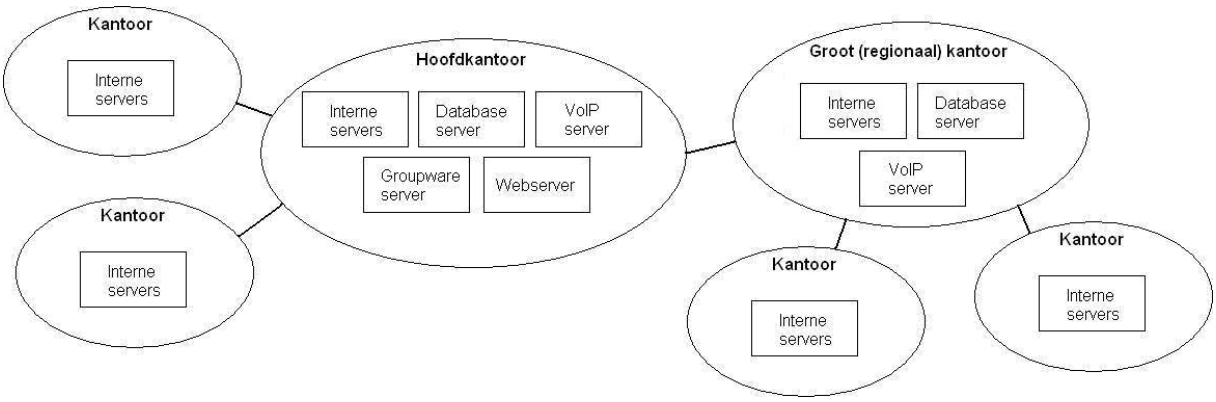
Kosten (in Euro's)	Installatie	Basisuitrusting	Maandelijks
Analoge modem	0	60-65	Gratis of forfaitair
ISDN	Vanaf 150	200	Vanaf 25
Kabel	150	250	35
ADSL	100	250	35 - 50
Frame-relay		2,000	Vanaf 50
Gedeelde T1		Vanaf 2,000	500 - 2,000
T3		Vanaf 20,000	6,000 - 30,000
Satelliet	Vanaf 200	400 - 3,500	Vanaf 70

3 Topologie

De WAN-topologie

Dit is ons idee over de topologie van de multinational, waarin onder meer de client-server structuur verwerkt zit. Als we ergens spreken over een server, betekent dit niet dat er fysiek maar n server aanwezig is, we duiden alleen aan dat die serverfunctie aanwezig is. Het is goed mogelijk dat een server is gemirrorred om de werkdruk per fysieke server te verlichten, of dat juist meerdere functies op n server, gentegreerd in n softwareoplossing zitten.

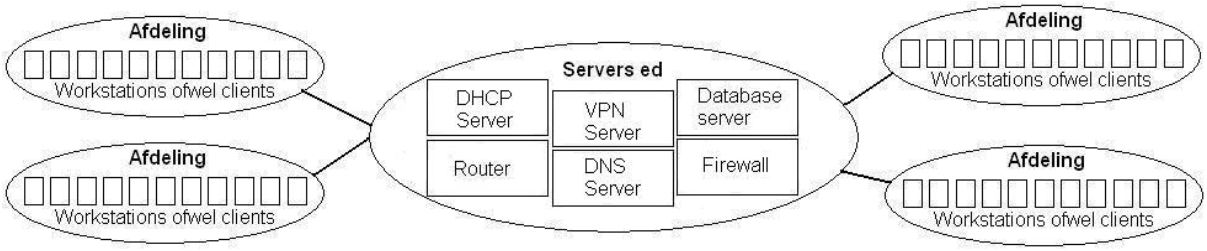
Het hoofdkantoor verzorgt enkele services die de andere kantoren niet hoeven te verzorgen. Dat de webserver centraal wordt geplaatst is vrij logisch, aangezien de multinational maar n website heeft en het niet nodig is dat ieder kantoor zijn eigen website heeft. Tevens wordt hierop de intranet, ofwel interne website, gehost. Er wordt ook centraal n groupwareserver gehost, waarop zich voor alle gebruikers onder andere een mailserver, newsserver en kalenderfunctie bevindt. De database wordt centraal geplaatst, maar elke vestiging heeft zijn eigen database waarop wordt gewerkt. Na werkuren synchroniseren de servers. Deze structuur is gekozen omdat het anders relatief veel geld gaat kosten om een server te kopen die honderden databasegebruikers tegelijk aankan en meestal de ene afdeling toch in een ander gedeelte van de database zit te werken dan de andere. Bijvoorbeeld de ene in de productenafdeling, de ander in productie, enz Als laatste hebben alle grote kantoren een VoIP-server om internettelefonie mogelijk te maken.



In termen van client-server zijn alle vestigingen client van de groupwareserver en webserver. De database-servers zijn allen zowel client als server van de centrale database-server, afhankelijk van de fase in het synchroniseerproces waarin ze zich bevinden. Wel is het zo dat kleine kantoren altijd client zijn van de database-server op de servers van de grote (regionale) kantoren, omdat ze zelf geen database server hebben, dit om de kosten te drukken en de servers beter te benutten. Om dezelfde redenen hebben de kleinere kantoren ook geen eigen VoIP-server.

LAN-topologie

In ieder kantoor zal de topologie er ongeveer zo uit komen te zien. Bij de workstations mag men ook VoIP-telefoons lezen.



Iedere afdeling staat in contact met een DHCP-server, die de IP-adressen aan de workstations toedeelt. Dit om de werkdruk op de systeembeheerders te verlichten en onderhoud aan het netwerk te versimpelen. Tevens staat er een router in elk kantoor om de toegang tot internet te regelen. Tevens bevat elk kantoor een VPN-server om onder andere thuiswerkers toegang te verschaffen tot alle services en bestanden op het netwerk, maar belangrijker nog om een virtueel intern netwerk te creren over de gehele wereld tussen alle vestigingen. Als laatste staat er ook in de kantoren die veel met databasegegevens werken een database-server, die werkt volgens het principe beschreven in de WAN-topologie. Ook krijgt elk kantoor een DNS-server om contact met andere nodes in het VPN-netwerk te versnellen en krijgt ieder kantoor een hardwarematige firewall om de beveiliging te vergroten.

4 Hardware

Binnen de multinational is het niet nodig om in n keer over te gaan op compleet nieuwe hardware. Het is beter om gebruik te maken van de bestaande hardware, en dat uit te breiden met nieuwe benodigde hardware. Het integreren van alle verschillende soorten hardware wordt gedaan door middel van de software, wat overal hetzelfde wordt.
Waarschijnlijk zijn er in de kantoren/productieafdelingen in onderontwikkelde landen niet veel computers, omdat er daar alleen een kantoor is gevestigd voor een goedkopere productie. Daar zijn dus niet zulke krachtige servers voor nodig, als die nog niet aanwezig zijn. Het gaat hier om een mailserver, een server voor de VoIP en een algemene server die zorgt voor de database, VPN, DNS en DHCP.
De krachtigere servers voor het hoofdkantoor moeten sowieso uitgebreid worden namelijk:

- Er moet namelijk een VoIP-server bijkomen, die er nog niet staat.

- De mailserver moet uitgebreid worden omdat het aantal werknemers door de fusie is gestegen en die hebben ook een back-up van hun mailbox op de centrale mailserver. Ook komt er nog een extra back-up mailserver op een fysiek andere plaats zodat iedereen nog bij zijn mail kan als de mailserver plat gaat.

- De algemene server(s) moet ook worden uitgebreid doordat de database in grootte toeneemt door de fusie. Binnen de gehele multinational willen we overgaan op VoIP in plaats van normale telefoon. Om alle normale toestellen te vervangen voor VoIP-toestellen gaat een beetje ver. Er is ook de mogelijkheid om een adapter aan je telefoon te koppelen zodat je de normale telefoon als VoIP-telefoon kan gebruiken. Zo is het ook niet nodig dat de werknemers aan een andere telefoon moeten wennen. Telefoons die later worden

toegevoegd binnen het bedrijf kunnen beter wel VoIP-toestellen zijn, want dat is wat goedkoper als een gewoon analoog toestel plus adapter.
Misschien zijn er nog verouderde computers in het netwerk. Omdat we binnen het hele bedrijf over willen gaan op Windows XP moeten de computers dus voldoen aan de systeemeisen van dit besturingssysteem. We willen een standaard maken voor de minimale systeemeisen, die steeds worden aangepast.

4.1 Kosten

De kosten voor hardware zullen alleen moeten worden gemaakt voor nieuwe servers, accelerators en firewalls, omdat een groot deel van het bestaande netwerk al geschikt is voor het nieuwe netwerk. Soms hoeft er alleen worden uitgebreid met nieuwe hardware.
De grootste kosten zullen gemaakt moeten worden voor de nieuwe servers. Prijsverschillen tussen verschillende servers zijn groot. Per locatie zal goed gekeken moeten wat er van een server verwacht wordt van bijvoorbeeld snelheid of schijfruimte. Servers die de capaciteiten hebben van een gewone PC kosten ook niet veel meer dan een gewone PC, dus minder dan duizend euro, maar als er krachtigere servers nodig zijn vaak servers tot een bedrag van 10000 euro geschikt. Verder kun je echte high performance servers natuurlijk zo duur maken als je zelf wilt.
De benodigde VPN accelerators (nodig om snelheidsverlies tegen te gaan bij gebruik van VPN over satelliet) zijn niet zo goedkoop. Deze apparaten kosten 1000 tot 3000 euro per stuk, maar ze hoeven alleen aangelegd te worden op plekken waar gebruikt gemaakt wordt van een satellietverbinding.
Voor de VPN software hoeft echter niets betaald te worden, omdat ze vaak gentegreerd zijn met softwarepakketten die al op de servers staan. Losse VPN software kan anders nog kosteloos gedownload worden van het internet.
Tenslotte zijn er nog de losse hardware firewalls, die in vele soorten te krijgen zijn. De kosten hiervan zijn vanaf 100,- en kunnen oplopen tot 1000,-.

5 Protocollen

Mailen
Voor de mail gebruiken we om te uploaden SMTP en voor het downloaden IMAP. We gebruiken IMAP voor de mapstructuur die dit protocol op de mailserver mogelijk maakt, waardoor je op elke locatie je mail/agenda/enz. kan opvragen. De satelliet verbinding is toereikend genoeg om goed gebruik te maken van dit protocol i.p.v. het POP3 protocol (wat aan het gebruik van een vast systeem gekoppeld is).

Netwerk
Voor communicatie over het netwerk gebruiken we het TCP/IP protocol omdat dit overal mee compatible is en dus makkelijk te installeren is binnen een complexe netwerk structuur, zoals in die van een multinational. Ook maakt ons systeem gebruik van het DHCP-protocol voor het automatisch toewijzen van de IP-adressen binnen ons netwerk.

Virtual Private Network
Hiervoor zullen we het protocol SSL gebruiken, de redenen hiervoor zijn:
- SSL is vrij eenvoudig te implementeren (t.o.v IPsec).
- SSL heeft een sterk beveilingsgehalte, wat zeer belangrijk is voor onze VPN verbindingen
- SSL is goed te gebruiken met de tunneling techniek die wij willen toepassen in ons netwerk.

Draadloos netwerk
De systemen die een draadloze verbinding hebben, communiceren d.m.v. het standaard gebruikte Wi-Fi protocol, namelijk het CSMA/CA protocol.

VoIP

We willen SIP als VoIP-protocol gebruiken omdat het het meest gebruikte protocol is voor voice-over-ip (dus betere ondersteuning). Ook is dit protocol makkelijk te implementeren omdat het een lichtgewicht protocol is.

6 Beveiliging

Mail / Encryptie
Als multinational is het belangrijk dat (belangrijke/vertrouwelijke) mailtjes niet in de handen van de verkeerde personen terecht komen (concurrenten bijvoorbeeld). Daarom is het van groot belang dat de mailtjes alleen te lezen door diefene voor wie ze bedoelt zijn. Daarom wordt alle mail bij dit bedrijf versleutelt. De encryptie van de mail gaat via de PGP (OpenPGP) standaard. Deze standard gebruikt een combinatie van symmetrische en a-symmetrische cryptografie. (is op college geheel uit de doeken gedaan)

Verbindingen
Naast de inhoudt van de mail is het ook belangrijk dat de verbinding van gebruiker naar server, of de verbindingen tussen de verschillende netwerken via een VPN, niet zomaar afgeluisterd kunnen worden. Dit voorkomen we door het boven op het TCP protocol het Secure Socket Layer protocol te gebruiken, dat alle data versleuteld voor transport. De versleuteling vind plaats via X.509 standaard, welke erg lijkt op PGP, en ook werkt met public/private keys. Het is de bedoeling dat deze (op termijn) vervangen wordt door PGP. Dus de SMTP/ IMAP/ POP3 verbindingen gaan allemaal versleuteld over het web, en wanneer mensen eventueel thuis hun mail/ data willen checken kan dat ook via HTTP over SSL (HTTPS).

Data
Afhankelijk van wat het belang van de data is, is het wellicht ook verstandig om bepaalde bestanden versleuteld op te slaan, zodat wanneer er fysiek ingebroken wordt, de data ook nog veilig is. Hiervoor gebruiken we een symmetrisch algoritme, met een sleutel gebaseerd op het wachtwoord van de gebruiker. Dit houdt natuurlijk ook automatisch in dat de wachtwoorden gebruikt binnen deze multinational moeten voldoen aan bepaalde voorwarden, om ze niet makkelijk te kunnen raden / kraken.

7 Software

De software voor dit netwerk zal alleen nodig zijn voor de servers en de nieuwe hardware die komt, aangezien de oude netwerken die al in de verschillende afdelingen aanwezig waren gewoon gebruikt worden. Als de oude netwerken niet compatibel zijn met de nieuwe structuur zullen ze vernieuwd worden en er zal Windows XP op gedraaid worden. Er is gekozen voor Windows XP, omdat de meeste mensen gewend zijn aan de Windows-omgeving en dit al hoogstwaarschijnlijk aanwezig is op de al in gebruik zijnde netwerken.

Voor de server op het hoofdkantoor is er de software SUSE Linux Enterprise Server 9. Er is hier voor gekozen, omdat het stabiel is en er zit gentegreerde beveiliging in, zoals een firewall en automatische monitoring en detectie van indringers. Ook zijn alle benodigde protocollen aanwezig. Het bevat bovendien applicatie- en databaseservices, zoals Apache, JBoss, Tomcat, MySQL en PostgreSQL, zodat er databases kunnen opgezet worden voor bijvoorbeeld producten, administratie en dergelijke dingen. Ook is er de mogelijkheid van virtuele privnetwerken aanwezig, waar ook voor gekozen is om gebruik van te maken. Verder is het opensource software, zodat er zonodig specifieke aanpassingen gemaakt kunnen worden.
Deze server fungeert ook als DNS-server, dit wordt ook ondersteund door de software, net zoals DHCP.

Voor de mailservers is er GroupWise 7 van Novell, die ook een goede beveiliging biedt en bescherming tegen, en detectie van virussen en spam. Het systeem biedt ook heel veel continuteit, in een onderzoek kwam uit dat 52 procent gebruikers hun GroupWise-systeem gedurende langer dan zes maanden niet opnieuw hadden hoeven opstarten, en 87 procent rapporteerde minder dan tien uur onvoorziene uitvaltijd per jaar.

Verder kan er gebruik gemaakt worden van Microsoft Outlook, dit wordt volledig ondersteund. Ook een agenda en kalender en gebruik als newsserver is mogelijk. Zo kan het hele bedrijf up-to-date gehouden worden.

Voor de VoIP is er gekozen voor GAO VoIP Software Solution, deze heeft ook ondersteuning voor fax en is betrouwbaar.

7.1 Kosten

De kosten van een SUSE Linux Enterprise Server 9-softwarepakket zijn ongeveer 250,- per licentie. Wanneer er veel licenties van een pakket gekocht worden, zal er natuurlijk korting worden gegeven. De kosten van een GroupWise 7 pakket, die gebruikt wordt op de mailservers, zullen per licentie rond de 60,- liggen.

8 Betrouwbaarheid

In de geest van betrouwbaarheid is het raadzaam op elke locatie eenzelfde soort hardware en software te gebruiken. Maar in dit probleem hebben veel locaties al werkende systemen, die waarschijnlijk niet identiek zijn; gelijkheid in gebruikte hardware is dus niet direct haalbaar (wel na verloop van tijd), maar gelijkheid in software wel direct.
Genstalleerde software op werkstations kunnen het beste op elk station identiek zijn. Dit garandeert uitwisselbaarheid tussen de verschillende locaties. Elke locatie kan het beste een back-up image van elke type werkstation van zijn locatie bijhouden, waarmee elk werkstation in korte tijd kan worden omgetoverd tot een schoon, werkend systeem waar alle nodige software op staat.
De betrouwbaarheid van de gekozen netwerkstructuur is voor het merendeel afhankelijk van de robuustheid van het VPN. Deze is opgebouwd door alle kantoren via het internet te verbinden. In het geval van uitval van het internet ligt er noodzakelijk ook (een deel van) het VPN plat, in het bijzonder dus ook de betrokken VoIP connecties. Hier is in beginsel weinig tegen te doen, maar de onbetrouwbaarheid van het internet is in veel gevallen sowieso wel kleiner dan die van het gewone telefoonnet.
Echter, in geval van onbereikbaarheid van delen van het VPN, mag er geen belangrijke data verloren gaan. Betrouwbaarheid van deze soort zit meestal al ingebakken bij de meeste professionele softwarepakketten die het bedrijf zou gebruiken; als de software vanwege de een of de andere reden een bewerking over het netwerk niet kan afmaken, zal het niet toestaan dat verzende, maar niet aangekomen informatie, verloren gaat.
Waar softwarepakketten geen invloed op hebben, is de betrouwbaarheid van de machines waar ze op werken.Van data moet gegarandeerd kunnen worden dat het intact en toegankelijk blijft. Ten tijde van een harddisk crash of een brand in een kantoor, moet het mogelijk zijn data zo snel mogelijk terug te kunnen zetten. Hiervoor zijn back-ups nodig.
Vanwege het feit dat het bedrijf zoveel kantoren over de wereld verspreid is, is het inefficint ervoor te kiezen alle data naar een centrale plek te zenden alwaar een back-up wordt gemaakt. Het is reler elk kantoor zijn eigen machines te laten back-uppen. Hiervoor moet het bedrijf duidelijke richtlijnen opstellen die door elk kantoor strikt worden opgevolgd. Een aanbeveling voor zulke richtlijnen is als volgt:

- Elke avond na werktijd wordt een back-up gemaakt van de werkdata van elke computer.
- De back-ups worden op tapes opgeslagen, en voor elke dag dat er een back-up wordt gemaakt dient er een vaste andere tape te worden gebruikt. De tapes worden opgeslagen op een fysiek beveiligde plaats, anders dan het kantoor zelf.
- Aan het eind van elke week wordt er van elke server (een computer die een of andere dienst levert aan het VPN, zoals een lokale bestellingendatabase) die in een kantoor aanwezig is, een volledige back-up gemaakt. Dit gebeurt op tape(s), of een externe harde schijf, afhankelijk van de hoeveelheid data op te slaan. Dit zodat in het geval van uitval van zon server, een vervangende server snel werkend te krijgen is door gebruik van deze volledige back-up. Een recente werkdata back-up kan vervolgens nog gebruikt worden om de data zover mogelijk te actualiseren.

- Het is handig minstens n keer per maand de back-ups te controleren op integriteit, en eventueel onbetrouwbare tapes te vervangen. Vervangen van tapes is sowieso nodig bij tapes die de maximale houdbaarheidsdatum gegeven door de leverancier halen.

9 Taakverdeling

De taken waren zoals in volgend tabel staat verdeeld. Het moet wel vermeld worden dat nagenoeg al het schrijven beinvloed is door het wekelijks groepsoverleg alwaar het een en ander werd besproken en van commentaar voorzien.

Hoofdstuk	Onderwerp	Auteur
2	Lijnen	Wesley
3	Topologie	Pieter
4	Hardware	Gerben
5	Protocollen	Stefan
6	Beveiliging	Chris
7	Software	Geerten
8	Betrouwbaarheid	Albert-Jan
2,4,7	Kosten	Jacob