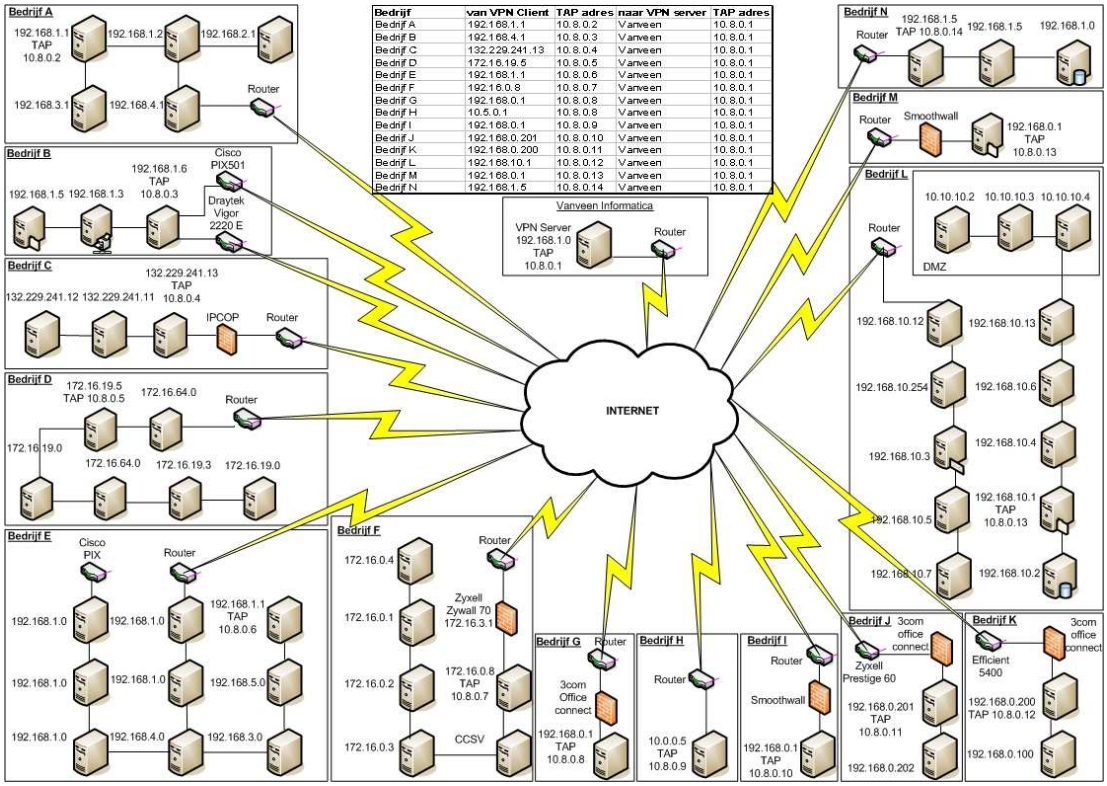
Afstudeerverslag

Het ontwerpen van een virtuele omgeving met daarbij gepaste monitoring software.

Onderzoek naar het vereenvoudigen van de huidige TI-situatie.



Bedrijf	van VPN Client	TAP adres	naar VPN server	TAP adres
Bedrijf A	192.168.1.1	10.8.0.2	Vanveen	10.8.0.1
Bedrijf B	192.168.4.1	10.8.0.3	Vanveen	10.8.0.1
Bedrijf C	132.229.241.13	10.8.0.4	Vanveen	10.8.0.1
Bedrijf D	172.16.19.5	10.8.0.5	Vanveen	10.8.0.1
Bedrijf E	192.168.1.1	10.8.0.6	Vanveen	10.8.0.1
Bedrijf F	192.168.0.8	10.8.0.7	Vanveen	10.8.0.1
Bedrijf G	192.168.0.1	10.8.0.8	Vanveen	10.8.0.1
Bedrijf H	10.5.0.1	10.8.0.8	Vanveen	10.8.0.1
Bedrijf I	192.168.0.1	10.8.0.9	Vanveen	10.8.0.1
Bedrijf J	192.168.0.201	10.8.0.10	Vanveen	10.8.0.1
Bedrijf K	192.168.0.200	10.8.0.11	Vanveen	10.8.0.1
Bedrijf L	192.168.10.1	10.8.0.12	Vanveen	10.8.0.1
Bedrijf M	192.168.0.1	10.8.0.13	Vanveen	10.8.0.1
Bedrijf N	192.168.1.5	10.8.0.14	Vanveen	10.8.0.1

Door Danny Spaans

Ter afronding van de studie Technische Informatica
aan de Haagse Hogeschool
in opdracht van
Vanveen informatica B.V.

Examinatoren:
Mevr. M.Nieuwland & Dhr. S. van Peski

Referaat

Danny Spaans, afstudeeropdracht, Het ontwerpen van een technische infrastructuur, Vanveen informatica, Zoetermeer, 12 januari 2007.

Dit document is beschreven in het kader van het project “Ontwerpen van een technische infrastructuur”. Dit project is, in de vorm van een afstudeerproject, onderdeel van de Haagse Hogeschool. Het afstudeerproject is uitgevoerd bij Vanveen informatica te Zoetermeer, gedurende de periode 4 september tot en met 12 januari.

Descriptoren:

- Afstudeeropdracht
- Afstudeerverslag
- Virtuele omgeving
- Virtual Private Network
- VPN
- Monitoring software
- Monitoring tools
- Netwerken
- Netwerkverbindingen
- ASI-Rapport
- Technische infrastructuur

Voorwoord

Dit is het verslag van het afstudeerproject van Danny Spaans in opdracht van de Haagse Hogeschool, uitgevoerd bij Vanveen informatica. Ter afsluiting van de opleiding Technische Informatica aan de Haagse Hogeschool is een afstudeerperiode van 90 dagen in het onderwijsprogramma opgenomen.

Mijn dank gaat uit naar mijn bedrijfsmentoren Dhr. C. Hogewoning en Dhr. R.J.J. Strijbos voor hun begeleiding en belangstelling.

Danny Spaans
Januari 2007

Inhoudsopgave

Lijst van figuren

Lijst van tabellen

1 Inleiding

Dit verslag is geschreven in het kader van de afstudeeropdracht die uitgevoerd is in opdracht van de Haagse Hogeschool, opleiding Technische Informatica. Dit verslag heeft als doel het duidelijk maken van de procesgang van de uitgevoerde opdracht. Hierbij is gelet op de keuzes die gemaakt zijn bij het tot stand komen van de producten en het resultaat van de ontwikkelingen.

Het primaire publiek van dit document zijn de examinatoren en de gecommitteerde welke de afstudeerperiode zullen beoordelen aan de hand van dit verslag. Verder is dit rapport geschreven voor mensen met een achtergrond in de technische informatica en die interesse hebben in mijn onderzoek naar een virtuele omgeving en het vinden van daarbij passende monitoring software.

2 Project

Dit hoofdstuk bevat de achtergrond informatie die bij de opdracht is beschreven. Daarnaast wordt de huidige situatie, probleemstelling, doelstelling en de op te leveren producten beschreven. Naar aanleiding van deze informatie ben ik tot de definitieve opdrachtomschrijving gekomen.

2.1 Het bedrijf

Vanveen informatica is een zelfstandige en onafhankelijke ICT-kennis-organisatie, actief vanaf 1987. Bij Vanveen informatica werken in totaal 37 mensen en bestaat uit 3 businessunits:
Internet Security Consultancy, Optional ICT-Support en Network & User Services.
De kerncompetenties van de organisatie liggen op het ontwikkelen, beheren en beveiligen van de infrastructurele kant van de ICT omgeving.

Internet Security Consultancy:
Bij Vanveen informatica zijn de consultants niet alleen in staat om een bedrijf te adviseren in de keuze van producten of inrichtingen daarvan, maar tevens ook in staat om deze operationeel te implementeren. Vervolgens hebben zij ook de specialisten in huis om de oplossingen te beheren.

Optional ICT-Support:
Vanveen informatica biedt ICT ondersteuning op maat aan, geheel passend bij de wensen en behoeften van het bedrijf. Desgewenst kan Vanveen informatica de zorg van een ICT-omgeving geheel op zich nemen. Vanveen informatica definieert samen met het bedrijf de mate waarin de ICT ondersteuning uitbesteed wordt in een ICT-zorgplan. De ondersteuning op maat ontstaat door het in kaart brengen van de verwachtingen van het bedrijf, het inventariseren van de bestaande ICT-omgeving en -processen, het uitwerken daarvan in het ICT-zorgplan, het implementeren van verbeteringen en het optimaliseren van het beheer.

Network & User Services:
Deze dienstverlening bestaat uit (project-)management, advies, ontwikkeling en implementatie. Met name heeft Vanveen informatica veel ervaring ten aanzien van het beheer, al dan niet conform ITIL, van complexe omgevingen. Ook kan de operationele gebruikersondersteuning worden verzorgd.

2.2 Huidige situatie

Vanveen informatica heeft een aantal bedrijfsnetwerken van midden en klein bedrijven onder remote beheer. Deze service valt onder de afdeling Optional ICT-Support. Momenteel wordt er via het internet een aparte connectie gemaakt naar het netwerk van een bepaald bedrijf via het remote desktop protocol(RDP) of Virtual Computing Network(VNC). Op deze manier kunnen de servers worden benaderd en kan bijvoorbeeld het event log worden geraadpleegd. Verder wordt de back-up gecontroleerd d.m.v. het bekijken van de log files en worden monitoring tools gebruikt die op de servers geïnstalleerd staan om de hardware te zoals harde schijven, het werkgeheugen, netwerkkaarten etc. te monitoren.

Er bestaan verschillende contracten met de bedrijven in welke mate het beheer moet worden uitgevoerd en wat voor ondersteuning er geleverd wordt. Zo kan het zijn dat de kleinere bedrijven een onderhoudscontract hebben afgesloten voor wekelijkse controles, terwijl de grote bedrijven, met grotere omgevingen, dagelijkse controles willen hebben en onderhoud aan hun systemen.

Al deze bedrijven beschikken over hun eigen omgeving met veelal verschillende hardware en software. De connectie die nu wordt gemaakt naar de server wordt toegelaten door de firewall die de poort van het RDP protocol of VNC toelaat van een bepaald IP adres vanaf het internet.

2.3 Probleemstelling

Elke dag worden er bedrijfsnetwerken gemonitored doormiddel van het remote beheer protocol. Via het internet wordt er verbinding gemaakt met een server en vervolgens wordt alles gecontroleerd. Omdat dit een dagelijks procedure is, is dit een methode die veel tijd in beslag neemt.

De diversiteit aan het hardware en software is groot. De back-upsoftware verschilt per bedrijf en heeft zo zijn eigen methode om logs te kunnen uitlezen of versturen. De monitoring software die op de servers zijn geïnstalleerd om de hardware te controleren, wijkt ook af per server en per bedrijf. Dit maakt het monitoren van de hardware en software onoverzichtelijk.

2.4 Doelstelling

Er zal onderzocht worden wat de beste oplossing is om een virtuele omgeving te creëren, waardoor alle bedrijfsnetwerken virtueel aan elkaar worden gekoppeld. Hierdoor kunnen alle bedrijfsnetwerken centraal gemonitored worden.

Het vinden van passende monitoring software voor het centraal monitoren van alle servers in de bedrijfsnetwerken.

2.5 Op te leveren producten

- Plan van aanpak
- Oriënterend Onderzoekrapport
- Architectuurdocument
- Ontwerpdocument
- Adviesrapport

2.6 Afbakening

De onderdelen die binnen het project vallen zijn:

- Het ontwerpen van een virtuele omgeving, tussen de verschillende bedrijfsnetwerken
- De virtuele omgeving moet toegankelijk zijn voor Vanveen
- Met een door mij geadviseerde monitoring tool moet het mogelijk zijn alle servers te monitoren conform de eisen van de opdrachtgever.

De onderdelen die buiten het project vallen:

- De beveiliging van de virtuele omgeving
- De implementatie van het ontwerp

Eisen:

- Alle bedrijfsnetwerken moeten binnen één virtueel netwerk zichtbaar zijn
- Bedrijven kunnen onderling niet op elkaars netwerk komen.
- Monitoring software moet op de gebruikte platformen inzetbaar zijn
- De monitoring software moet gelijktijdig alle servers van de bedrijfsnetwerken kunnen controleren op de netwerkbeschikbaarheid, hardware(geheugen, harde schijven, processors etc.), Windows event logs en back-up logs
- De software bij klanten mag niet functioneel gewijzigd worden
- Er mogen geen hardware aanpassingen komen bij klanten.

3 Definitiefase

In de definitiefase wordt als eerste een duidelijk beeld gevormd van de huidige situatie. Als de huidige situatie in kaart is gebracht kan de probleemstelling, doelstelling en de eisen en wensen worden opgesteld. Bovendien wordt er onderzocht welke methode het best toegepast kan worden voor dit project. Vervolgens zal het plan van aanpak worden opgesteld.

Verder wordt er in deze fase onderzocht met welke type netwerkverbindingen een virtuele omgeving gerealiseerd kan worden en met welke monitoring software deze virtuele omgeving gemonitored kan worden. Ook wordt er een inventarisatie gemaakt van de hardware, software en IP-adressen van klanten. Deze resultaten zullen worden beschreven in een oriënterend onderzoeksrapport. Dit document is bedoeld als informatiebron waar in de volgende fases naar teruggekoppeld kan worden.

In de volgende fase worden er keuzes gemaakt tussen de onderzochte resultaten. In deze fase wordt er alleen onderzocht, maar er worden nog geen keuzes gemaakt.

3.1 Huidige situatie in kaart brengen

De eerste activiteit van het afstudeerproject is een duidelijk beeld vormen van de huidige TI-situatie. Dit is nodig om te constateren, waarom de huidige situatie niet voldoet aan eisen van de opdrachtgever en waarom de opdrachtgever wilt dat er onderzoek wordt gedaan naar een nieuwe TI-situatie. Om dit beeld te vormen heeft er een gesprek plaats gevonden met de opdrachtgever. Tijdens dit gesprek heeft de opdrachtgever verteld, dat de bedrijfsnetwerken gemonitored worden doormiddel van het remote desktop protocol(RDP) of virtual computing network(VNC). Met behulp van RDP of VNC worden de servers overgenomen en worden verschillende logbestanden, de netwerkbeschikbaarheid en hardware gecontroleerd. Ook werd duidelijk dat er rekening gehouden moest worden met de huidige situatie. De software van klanten mag niet functioneel gewijzigd worden en er mogen geen hardware aanpassingen komen.

Vervolgens heb ik de volgende vragen gesteld:

- Welke log bestanden worden er gemonitored?
- Welke hardware dient er gemonitored te worden?
- Welke besturingsystemen komen in de bedrijfsnetwerken voor?

De logbestanden die gemonitored moeten worden zijn de Windows event logs, Linux syslogs en de back-upsoftware logs. Van de hardware is het belangrijk dat de processor, geheugen en harde schijf gecontroleerd wordt. Bij de klanten komen zowel Linux als Windows systemen voor.

Als laatste heb ik een afspraak gemaakt met een medewerker van de afdeling Optional ICT-Support(OIS), die bedrijfsnetwerken monitored. Hij gaf een demonstratie, hoe de

bedrijven in de huidige situatie gecontroleerd worden. Hierdoor heb ik een nog beter beeld gekregen van de huidige situatie.

3.2 Ontwikkel strategie kiezen

Een belangrijk aspect van het ontwerpen van een technische infrastructuur (TI) is het kiezen van een gepaste methode. Het toepassen van een methode is noodzakelijk om gestructureerd te kunnen werken.

Ik heb onderzoek gedaan naar de methoden PRINCE2 en ASI-rapport of deze toepasbaar zijn voor dit project, omdat ik met beide methoden heb ik al eerder kennis gemaakt gedurende mijn opleiding.

PRINCE2 is een methode die toepasbaar is op alle projecten en kent een grote flexibiliteit. Aspecten van de methode die niet van toepassing zijn op (of niet nuttig voor) een bepaald project, kunnen overgeslagen worden.

ASI-rapport is een methode die een gefaseerde aanpak gebruikt, specifiek voor het ontwerpen van een TI. Deze methode is net als PRINCE2 flexibel, omdat het de ontwikkelaar vrij laat om de methode aan te passen naar eigen behoefte. Omdat de aspecten binnen de PRINCE2 methode niet specifiek bedoeld zijn voor het ontwerpen van TI vond ik ASI-rapport beter geschikt, omdat deze hier wel specifiek voor bedoeld is.

Het ontwerp wordt niet geïmplementeerd, omdat de implementatie geen onderdeel is van de afstudeeropdracht daarom heb ik de ontwikkelfase buiten beschouwing gelaten. Wel heb ik het testplan, wat een activiteit is binnen de ontwikkelfase opgenomen in de ontwerpfase. Dit heb ik gedaan omdat het ook belangrijk is dat de voorkeuroplossing getest wordt, om te constateren of het daadwerkelijk de gewenste resultaten oplevert. Als blijkt dat het onderzoek niet het gewenste resultaat op levert dan dient er een oplossing gevonden te worden en anders wordt er verder gewerkt met de alternatieve oplossing.

In de definitiefase is een oriënterend onderzoeksrapport toegevoegd. Dit is geen officieel document van het ASI-rapport, maar omdat er in deze fase veel onderzocht wordt, hebben mijn medestudent en ik besloten om een oriënterend onderzoeksrapport toe te voegen. Hierin staan alle onderzoeksresultaten die tijdens de definitiefase vergaard zijn en wordt als naslagwerk gebruikt, zodat er in de volgende fases teruggekoppeld kan worden.

3.3 Het opstellen van het plan van aanpak

Het plan van aanpak is het eerste product wat opgeleverd wordt in de definitiefase. Hierin zijn de huidige situatie, doelstelling, probleemstelling en eisen en wensen opgesteld. Verder wordt beschreven welke methode in dit project wordt gehanteerd en welke activiteiten geselecteerd zijn voor dit project. Daarna is de opdrachtomschrijving en werkwijze opgesteld.

Ook is er een planning opgesteld. De planning geeft een overzicht van alle activiteiten die per week plaats vinden gedurende het project. Bovendien zijn de drie fases van het ASI-rapport in de planning opgenomen, dit geeft een overzicht is van in welke week een fase begint of eindigt. Hier volgt een overzicht van mijn planning.

Tabel 3-1 Planning

Week	Fase	Startdatum/einddatum	Activiteiten
1	Definitiefase	4-9-2006/8-9-2006	- Kennismaken - Huidige situatie bekijken - Opstellen deel van pva
2	Definitiefase	11-9-2006/15-9-2006	- Eerste concept pva inleveren - Onderzoeken naar de mogelijkheden om een virtuele omgeving te creëren
3	Definitiefase	18-9-2006/22-9-2006	- Onderzoeken naar de mogelijke type VPN-verbindingen - Pva final inleveren
4	Definitiefase	25-9-2006/29-9-2006	- Onderzoeken naar de mogelijke type VPN-verbindingen - De gevonden mogelijkheden documenteren - pva verbeteren en verder uitbreiden
5	Definitiefase	2-10-2006/6-10-2006	- Onderzoek naar beschikbare monitoring tools. - bevindingen documenteren
6	Definitiefase	9-10-2006/13-10-2006	- Onderzoek naar beschikbare monitoring tools. - Bevindingen documenteren - Oriënterend onderzoeksrapport inleveren
7	Architectuurfase	16-10-2006/20-10-2006	- Gesprek met examinatoren - Keuzes maken van de onderzochte resultaten
8	Architectuurfase	23-10-2006/27-10-2006	- Keuzes maken van de onderzochte resultaten - Definitieve opdrachtomschrijving inleveren
9	Architectuurfase	30-10-2006/3-11-2006	- Voorkeursoplossingen verder uitwerken - Onderzoeken welke eventuele hardware aangeschaft moet worden - Voortgang verslag inleveren voor school
10	Architectuurfase	6-11-2006/10-11-2006	- IP-adressering bepalen van de nieuwe situatie - Blauwdruk(tekening) ontwerpen van de nieuwe netwerk infrastructuur
11	Architectuurfase	13-11-2006/17-11-2006	- Blauwdruk(tekening) ontwerpen van de nieuwe netwerk infrastructuur
12	Ontwerpfase	20-11-2006/24-11-2006	- Inleveren concept architectuurdocument
13	Ontwerpfase	27-11-2006/1-12-2006	- Virtuele omgeving simuleren en testen

14	Ontwerpfase	4-12-2006/8-12-2006	- Virtuele omgeving simuleren en testen - gedetailleerde bouwplan inleveren voor school
15	Ontwerpfase	11-12-2006/15-12-2006	- Testen van de monitoring tool via de virtuele omgeving
16	Ontwerpfase	18-12-2006/22-12-2006	- Testen van de monitoring tool via de virtuele omgeving - inleveren ontwerpdocument
17	Ontwerpfase	2-1-2006/5-1-2006	- Afronden afstudeerverslag - Presentatie maken
18	Ontwerpfase	8-1-2006/12-1-2006	- inleveren adviesrapport - Presentatie presenteren aan het personeel afstudeerverslag inleveren

Als laatste zijn de mijlpalen opgesteld, hierin staat in welke week en fase een product opgeleverd wordt. Hier is het overzicht van de mijlpalen.

Tabel 3-2 Mijlpalen

Week	Fase	Op te leveren documenten
3	Definitiefase	Plan van aanpak
8	Definitiefase	Onderzoeksrapport, definitieve opdrachtomschrijving
12	Architectuurfase	Architectuurdocument
15	Ontwerpfase	Ontwerpdocument
18	Ontwerpfase	Adviesrapport, presentatie, afstudeerverslag

3.4 Opstellen van het oriënterend onderzoeksrapport

In het oriënterend onderzoeksrapport worden alle onderzoeksresultaten die tijdens de definitiefase vergaard zijn opgesteld en wordt als naslagwerk gebruikt, zodat er in de volgende fases naar teruggekoppeld kan worden. De onderzoeksresultaten zijn hieronder kort beschreven. Voor alle onderzoeksresultaten zie de B

3.4.1 Onderzoek naar de type VPN-verbindingen en gebruikte technieken

Ik wist dat een virtuele omgeving gerealiseerd kan worden met VPN-verbindingen, maar hoe dat toegepast kan worden in de huidige situatie wist ik niet. Met een VPN wordt bedoeld dat er een koppeling is tussen netwerken via het publieke internet door middel van tunnels, waarbij de netwerken als één groot netwerk functioneren. Ook wist ik dat er verschillende typen VPN-verbindingen zijn, maar ook hierin was mijn kennis beperkt. Hierdoor heb ik mijn wat meer verdiept in VPN door op internet te onderzoeken welke typen VPN-verbindingen er zijn en welke technieken ze gebruiken bij het maken van een verbinding. Bij dit onderzoek heb ik rekening moeten houden met mijn collega die de beveiliging onderzoekt, want beveiliging is een onderdeel van VPN. De VPN-verbindingen die niet beveiligd kunnen worden heb ik niet verder onderzocht. Dit onderzoek heeft geresulteerd in de volgende type VPN's en technieken.

- IPSec(Internet Protocol Security)
- MPLS(Multi Packet Layer Switching)
- PPTP(Point to Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- OpenVPN

IPSec

De IPSec-tunnelmodus is vooral bedoeld voor het beschermen van het verkeer tussen diverse netwerken wanneer dit verkeer via een tussenliggend, niet-vertrouwd netwerk loopt. De tunnelmodus wordt voornamelijk gebruikt ten behoeve van interoperabiliteit met gateways, of eindsystemen die geen L2TP/IPSec- of PPTP-verbindingen ondersteunen.

MPLS

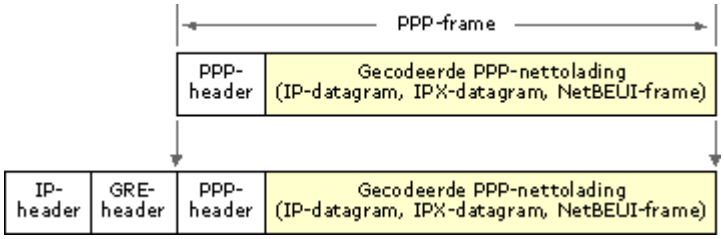
Bij MPLS worden er labels toegekend aan de datapakketjes, zodat het switchen en routeren van de pakketjes sneller gaat. Het nadeel van deze VPN-verbinding is dat er weinig goedkope hardware beschikbaar is die deze VPN-verbinding ondersteunt.

PPTP

PPTP is een uitbreiding van Point-to-Point Protocol (PPP) waarin wordt voortgebouwd op de verificatie-, compressie- en coderingsmechanismen van PPP.
PPTP en MPPE (Microsoft Point-to-Point Encryption) verschaffen de primaire VPN-services voor de inkapseling en codering van persoonlijke gegevens.

Inkapseling:
Een PPP-frame (een IP-, IPX- of Appletalk-datagram) wordt verpakt met een GRE-header (Generic Routing Encapsulation) en een IP-header. In de IP-header bevinden zich het bron- en het doel-IP-adres die bij de VPN-client en VPN-server horen.

Figuur 3-1 Inkapseling PPP frame



PPTP maakt gebruik van TCP poort 1723. PPTP werkt vrij vlot, maar laat de wensen over op het gebied van beveiliging.

L2TP

Layer Two Tunneling Protocol (L2TP) is een op een RFC2341 en RFC2637 gebaseerd tunnelprotocol dat is uitgegroeid tot een industrienorm. In tegenstelling tot PPTP maakt L2TP op servers waarop Windows Server 2003 wordt uitgevoerd geen gebruik van Microsoft Point-to-Point Encryption (MPPE) om Point-to-Point Protocol (PPP)-datagrammen te coderen. L2TP is afhankelijk van IPSec (Internet-protocolbeveiliging) voor coderingsservices. De combinatie van L2TP en IPSec wordt aangeduid met L2TP via IPSec. L2TP via IPSec verschaft de primaire VPN-services voor de inkapseling en codering van persoonlijke gegevens.

Inkapseling voor L2TP-via-IPSec-pakketten bestaat uit twee lagen.
- L2TP-inkapseling
- IPSec-inkapseling

OpenVPN

OpenVPN is een VPN softwarepakket wat de mogelijkheid heeft om point-to-point encrypted tunnels tussen hosts op te zetten. OpenVPN opereert op laag 2 of 3 van het OSI-model door middel van het SSL/TLS protocol en heeft verschillende authenticatie mogelijkheden.

3.5 Systeem monitoring software

Bij het eerste gesprek met de opdrachtgever is er naar voren gekomen welke eisen er worden gesteld aan de monitoring software. Aan de hand van deze eisen zijn er selectiecriteria opgesteld.

- Monitoren van Windows en Linux systemen
- Installatie op Windows en/of Linux
- Monitoren van de netwerkbeschikbaarheid
- Monitoren van hardware
- Monitoren van Windows event logs
- Monitoren van Linux syslogs
- Monitoren van back-up software logs
- Goede ondersteuning van de producent / open source comunity
- Mogelijkheid tot het uitbreiden van de opties

Tijdens het zoeken naar monitoring tools ben ik op de volgende site belandt http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html. Hier staan tientallen monitoring tools voor het monitoren van netwerken. Op alle monitoring tools die op site vermeld staat heb ik de selectiecriteria toegepast. Dit heeft geresulteerd in de volgende monitoring tools.

- Big Brother
- Big Sister
- Microsoft Operations Manager(MOM)
- Nagios
- Zabbix
- MonitorMagic

Van deze monitoring tools heb ik in het kort beschreven wat de mogelijkheden van hier van zijn. Deze informatie heb ik op de website gevonden van de monitoring tools in kwestie. De websites zijn terug te vinden in hoofdstuk 7 “Literatuurlijst”. De beschrijving van de monitoring tools is te vinden vanaf de volgende bladzijde.

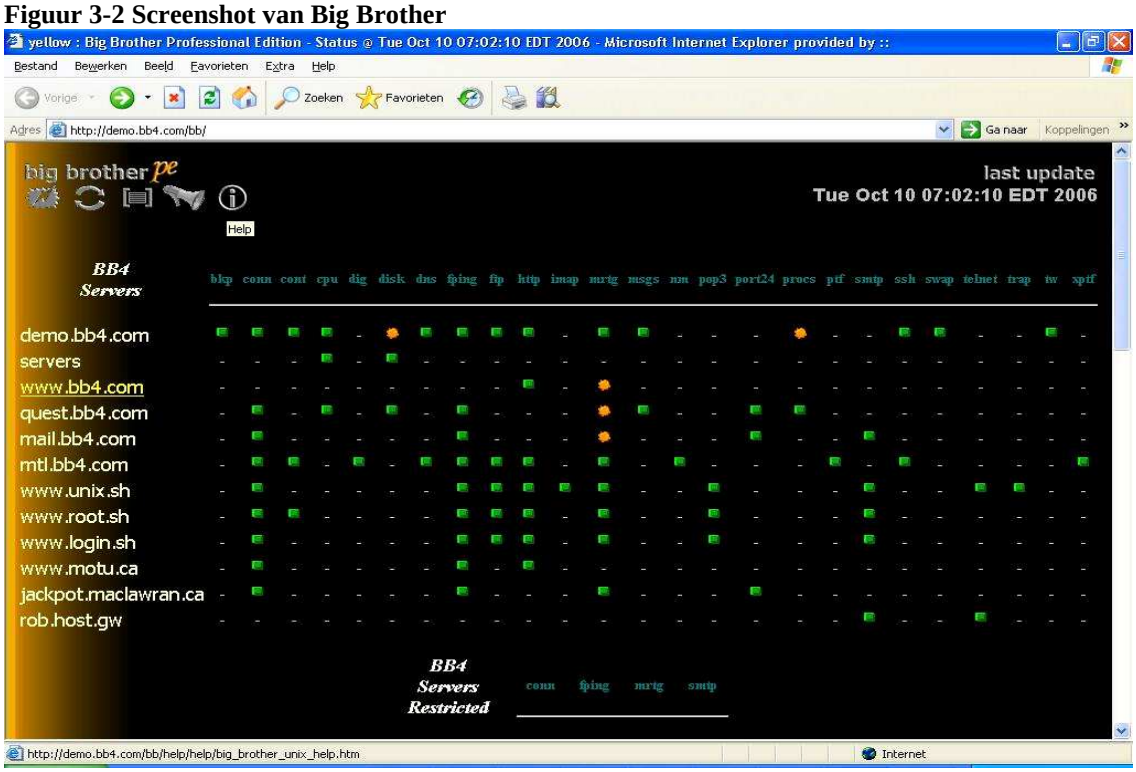
Big Brother

Big Brother is een website gebaseerde monitoring tool, die de mogelijkheid bied om de beschikbaarheid van zowel Windows als Linux computers te monitoren.

Deze monitoring tool bestaat uit een server– en client installatie. De server is voorzien van een database en hierop worden alle gegevens opgeslagen. Het controleert ook netwerkenprotocollen zoals o.a. FTP, HTTP, POP3.
De client controleert hardware gegevens zoals o.a. de processor, geheugen en schijfruimte, Linux syslogs en Windows event logs. Deze hardware gegevens worden naar de server gestuurd. Deze tool kan zowel op Linux als Windows systemen geïnstalleerd worden.

Er bestaat ook een gebruikers gemeenschap waar gebruikers hun zelf gemaakte scripts naar toe kunnen sturen(www.deadcat.net). Dit zijn scripts om bijvoorbeeld back-up software logs te monitoren, wat standaard niet mogelijk is. Door deze script erbij toe te voegen biedt het deze mogelijkheid wel. Er is ook de garantie dat als er een script nodig is die niet in de gemeenschap voorkomt, dat Big Brother die binnen 30 dagen ontwikkelt.

Figuur 3-2 Screenshot van Big Brother



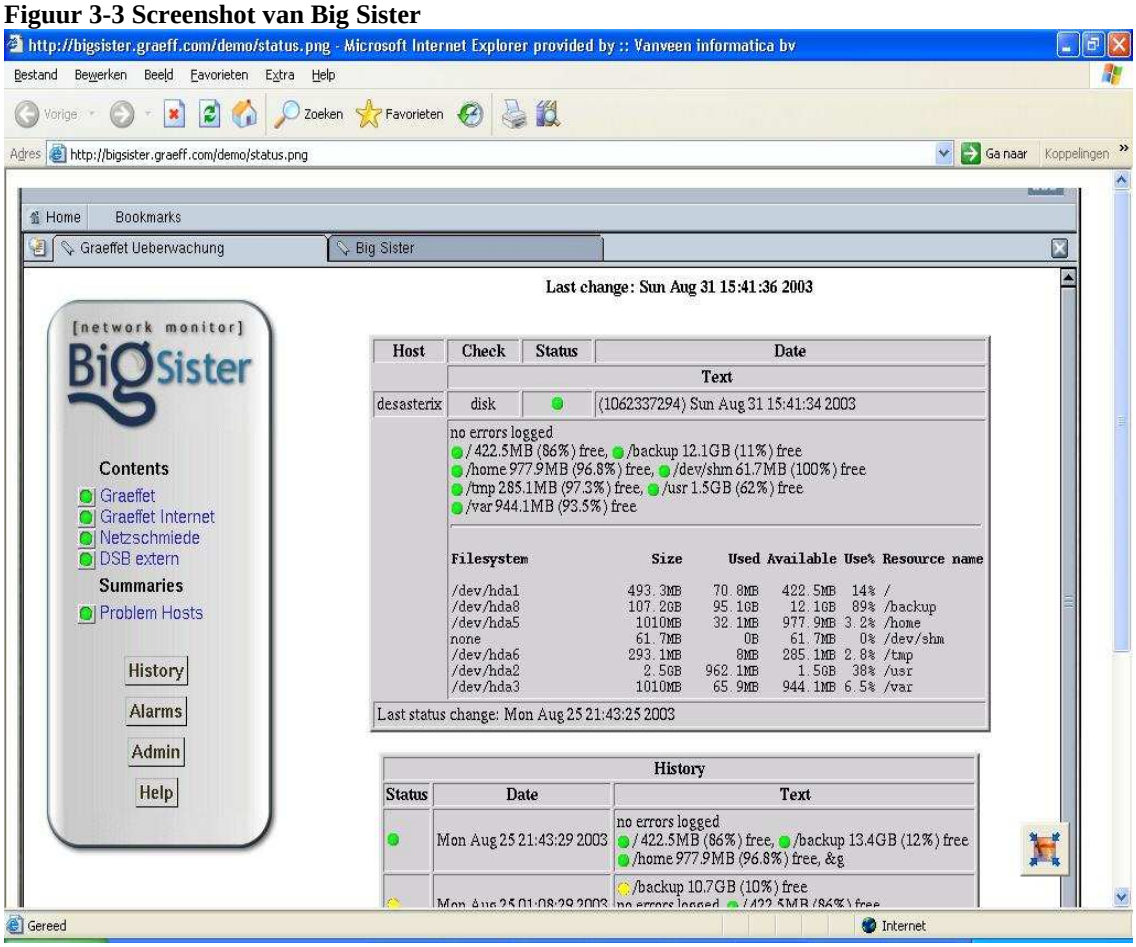
Big sister

Big Sister is een open source, website gebaseerde monitoring tool, die de beschikbaarheid van netwerken controleert. Open-source software betekent dat de bron code is gepubliceerd en vrij beschikbaar is voor het publiek, waardoor iedereen het vrij kan kopiëren, aanpassen en herverspreiden zonder kosten aan auteursrechten en toeslagen. De ontwikkeling van open-source code gebeurt door gemeenschappelijke samenwerking van zowel individuele programmeurs als grote bedrijven

Deze tool kan zowel op Linux als Windows computers geïnstalleerd worden. Ook kan het beide platformen monitoren. De software bestaat uit een server en een agent. Het centrale gedeelte is de server en deze is voorzien van een database en monitored de beschikbaarheid van computers. De agent kan hardware van de servers en werkstations monitoren zoals, de processor, het geheugen, netwerkkaarten etc. De status informatie van deze hardware wordt verstuurd naar de server en wordt in de database opgeslagen. Problemen die zijn geconstateerd kunnen door e-mail of SMS weergegeven worden.

Ook Big Sister heeft de mogelijkheid om externe scripts toe te voegen zodat het mogelijk is om bijvoorbeeld back-up software logs te controleren.

Figuur 3-3 Screenshot van Big Sister

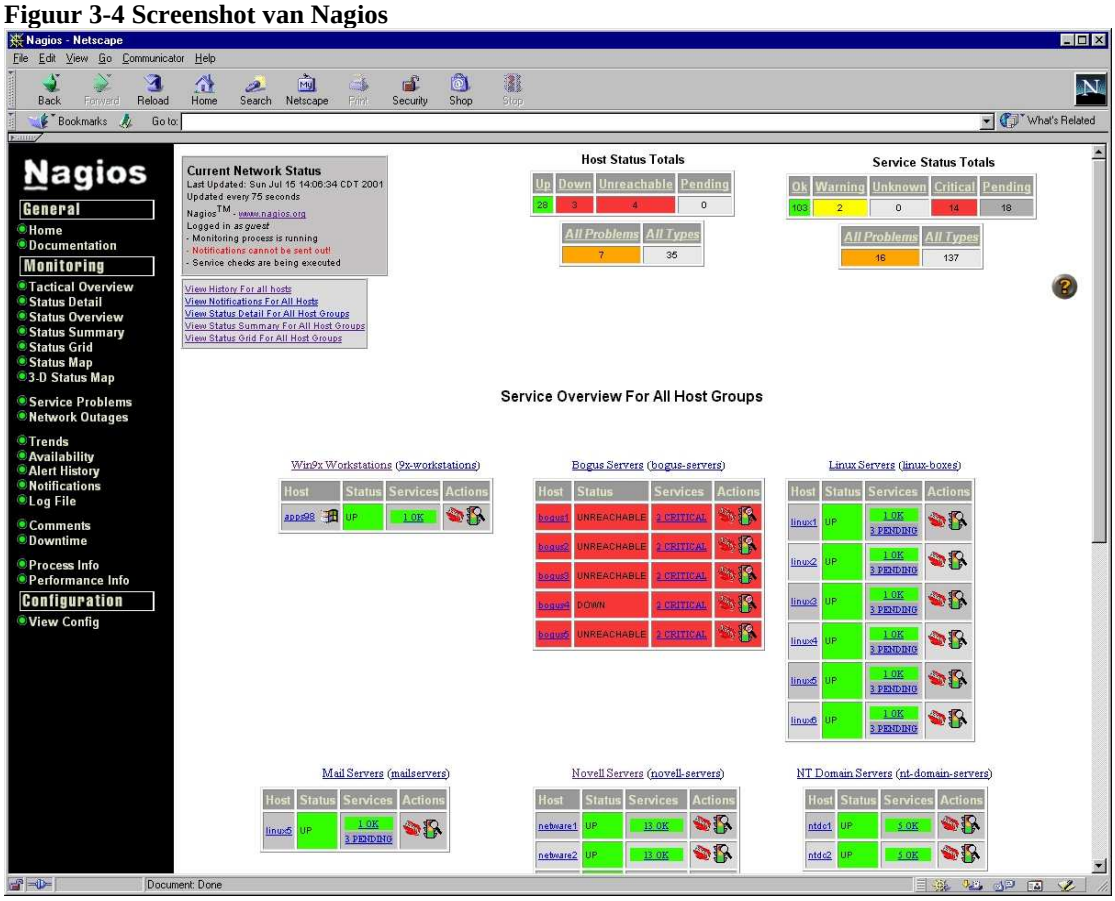


Nagios

Nagios is een open-source website gebaseerde netwerk monitoring tool, die alleen op Linux is te installeren. De tool controleert de netwerkbeschikbaarheid van hosts. Door gebruik te maken van externe plug-ins, kunnen alle hosts en services zelf worden ingesteld. Deze plug-ins worden geïnstalleerd op de clients en daarbij kan ingesteld worden dat het hardware en Linux event logs worden gemonitored.

Het monitoren van het Windows besturingssysteem wordt standaard niet ondersteund. Hierdoor is het niet mogelijk om hardware, event logs, back-up van Windows systemen te monitoren. Wel biedt Nagios de mogelijkheid om daarvoor zelf een plug-in voor te schrijven. De plug-ins kunnen geschreven worden in de talen C, Shell, Perl en Python.

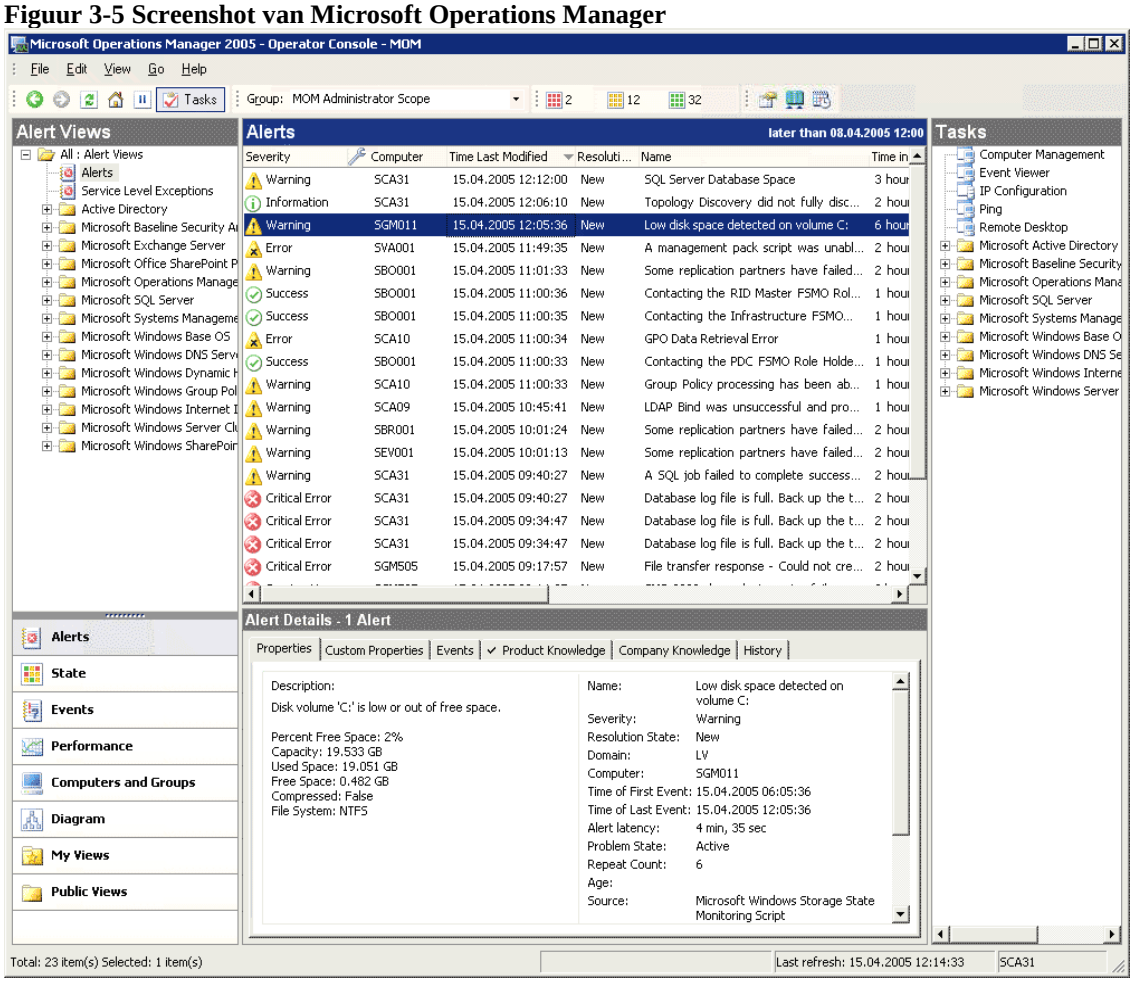
Figuur 3-4 Screenshot van Nagios



Microsoft Operations Manager (MOM)
MOM maakt het mogelijk de door Windows systemen in log bestanden vastgelegde events te analyseren. Met behulp van speciale, door Microsoft ontwikkelde, intelligente scripts (verzameld in Management Packs), is MOM in staat om alerts (waarschuwingsboodschappen) te genereren.

Er zijn ook management packs beschikbaar die het mogelijk maken om Linux systemen te monitoren. Hiermee is het mogelijk om de Linux hardware en syslogs te monitoren. Op de site van microsoft kan er een development guide gedownload worden, waarmee zelf management packs gemaakt kunnen worden om bijvoorbeeld back-upsoftware te monitoren.

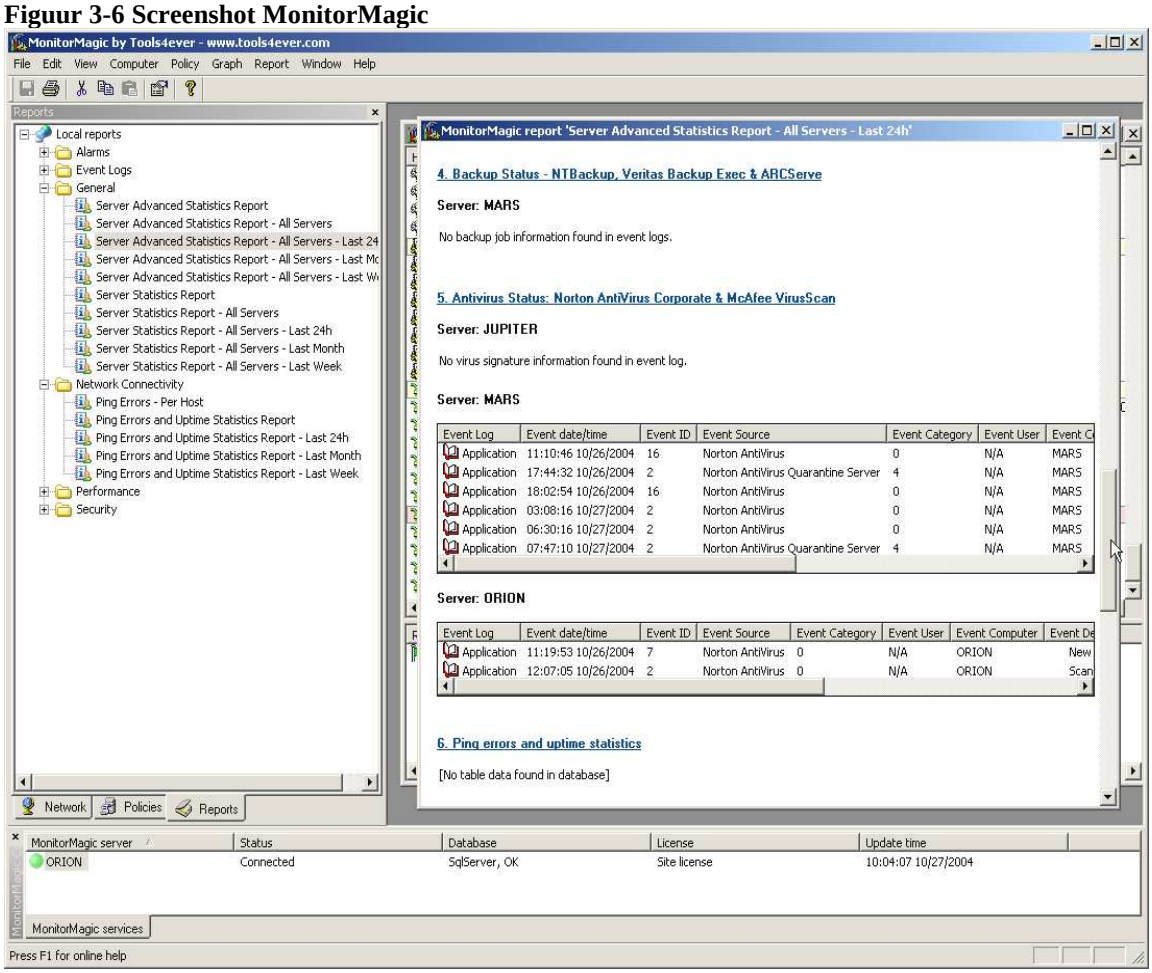
Figuur 3-5 Screenshot van Microsoft Operations Manager



MonitorMagic

MonitorMagic is een pro actieve monitoring en beheer oplossing voor Windows platformen. Met deze software is het mogelijk om de netwerkbeschikbaarheid van computers te controleren. Ook kan het hardware en Windows event logs monitoren. Het is ook mogelijk om Linux systemen te monitoren met behulp van het SNMP(Simple Network Management Protocol) protocol. SNMP is een protocol dat werkt over een TCP/IP netwerk voor het verkrijgen van informatie van systemen die op het TCP/IP netwerk zijn aangesloten. Het is ook mogelijk om met MonitorMagic back-up software logbestanden te controleren zonder daarbij een plug-in te installeren. Het kan alleen op Windows besturingsystemen geïnstalleerd worden..

Figuur 3-6 Screenshot MonitorMagic



Zabbix

Zabbix is een open source, web gebaseerde monitoring software voor het monitoren van applicaties en servers. Het kan alleen geïnstalleerd worden op Linux systemen, wel kan het beide platformen monitoren.
De software bestaat uit een Zabbix server en een Zabbix agent. Het centrale gedeelte is de Zabbix server en deze is voorzien van een database. De Zabbix agent kan hardware van de servers en werkstations optimaal monitoren zoals, de processor, het geheugen, netwerkkaarten etc. De status informatie van deze hardware wordt verstuurd naar de Zabbix server en wordt in de database opgeslagen. Met behulp van een webbrowser kan er gemonitored worden.

Het monitoren van applicaties wordt aangeboden, maar het monitoren van o.a. back-up software, Windows event logs zitten standaard niet bij het pakket. Het is door middel van een shell script, wel mogelijk om deze applicaties te monitoren.

Figuur 3-7 Screenshot Zabbix

3.6 Inventarisatie van hardware, software en IP-adressen van klanten

Om te controleren of het wel mogelijk is om gebruik te maken van VPN bij de klanten, is er een inventarisatie gemaakt van bepaalde hardware en software van klanten. De IP-adressen zijn belangrijk voor de volgende fase, als er een keuze wordt gemaakt welk virtueel IP-adres er gebruikt gaat worden. De inventarisatie is weggelaten uit de bijlage in verband met vertrouwelijke informatie.

De informatie van klanten is geplaatst in een beveiligde map op de server, maar omdat ik moest achterhalen welke hardware, software en IP-adressen de klanten gebruiken, heb ik daarop toegangsrechten gekregen. Deze informatie was niet altijd volledig en goed bijgehouden, hierdoor is het heel onoverzichtelijk voor mij geweest, om te constateren welke hardware, software of IP-adressen er gebruikt worden. Als er van de informatie van een klant iets niet duidelijk is, ben ik naar een medewerker van de afdeling OIS gegaan die het bedrijf in kwestie beheert en mij de informatie kon geven die ik nodig had.

Omdat niet alle hardware en software essentieel is, heb ik de volgende selectiecriteria opgesteld van de hardware en software die wel relevant zijn. Hieronder staan selectiecriteria en waarom deze geselecteerd zijn.

- **Routers en firewalls**

Als er wordt gekozen voor een VPN-verbinding die door routers afgehandeld wordt, betekent dit dat elke klant een router dient te hebben. Hierom wordt er gecontroleerd of elke router of firewall bij een klant een VPN-verbinding ondersteunt.

- **Server hardware en besturingsysteem**

Als er wordt gekozen voor een VPN-verbinding die door servers afgehandeld wordt, dan is het belangrijk om te weten of de huidige hardware en het besturingsysteem dit ondersteund

- **Back-up software**

Een eis van de opdrachtgever is dat de back-up logs gecontroleerd moeten worden Hiervoor heb ik ook gecontroleerd welke back-up software aanwezig is bij klanten. Als er wordt gekozen voor een monitoring tool, kan er gekeken worden of het de back-up software ondersteunt.

- **IP-adressen**

Een VPN-verbinding maakt gebruik van virtuele IP-adressen. Dit zijn privé IP-adressen die ook worden gebruikt voor lokale netwerken. Het virtueel IP-adres dient anders te zijn dan het lokale netwerkadres, anders kunnen IP-adres conflicten ontstaan. Hierom worden ook de privé IP-adressen van de klanten geïnventariseerd.

4 Architectuurfase

De architectuurfase heeft tot doel de globale structuur te vormen voor de uiteindelijke TI. Dit wordt gedaan door eerst een keuze te maken wat de beste methoden is om de nieuwe TI situatie te realiseren. ASI-rapport beschrijft dat er een voorkeursoplossing en alternatieve oplossingen op moeten worden gesteld. Hierdoor heb ik keuzes gemaakt tussen verschillende onderdelen van de onderzochte resultaten in definitiefase. Vanwege de beperkte duur van deze fase heb ik er voor gekozen om één alternatieve oplossing te selecteren voor een VPN-verbinding en een monitoring tool. Vervolgens worden de oplossingen verder uitgewerkt en kan de netwerktekening worden opgesteld. De resultaten van dit onderzoek zijn opgesteld in het architectuurdocument.

4.1 Methoden om een virtuele omgeving te creëren

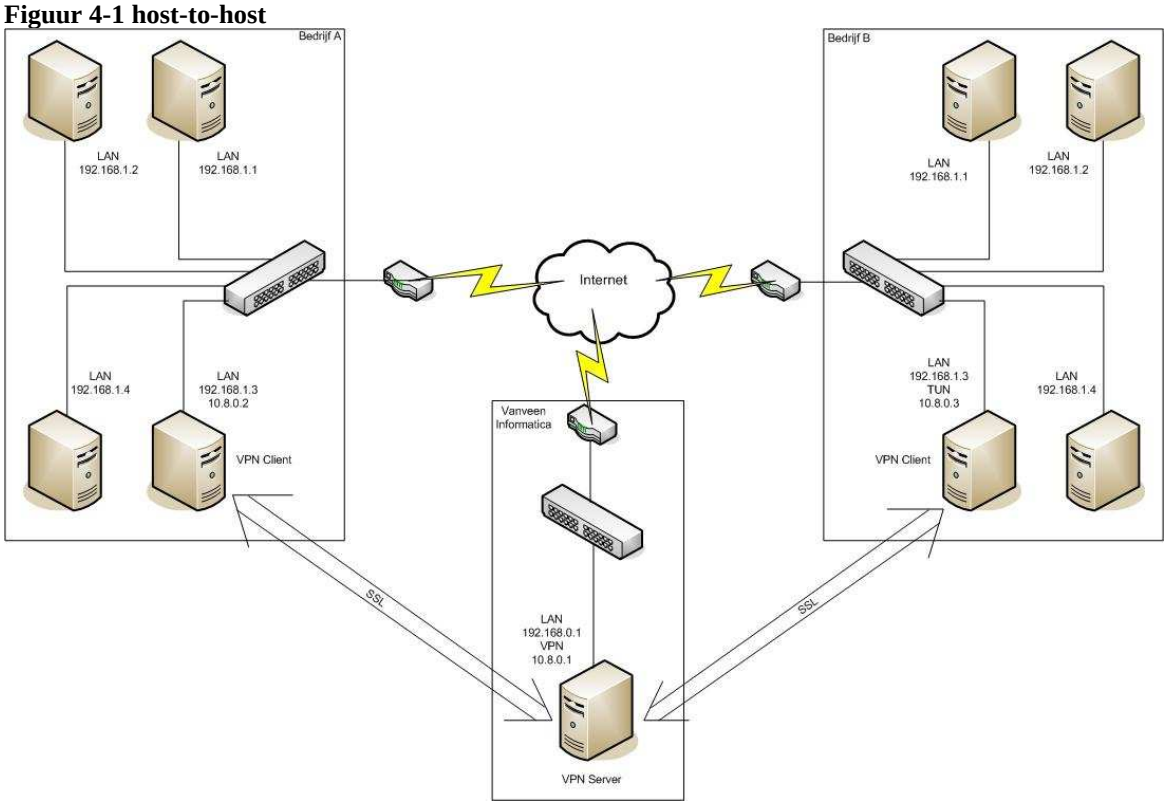
In het oriënterend onderzoek is gebleken dat er drie methodes zijn waarmee een virtuele omgeving gerealiseerd kan worden. Ik heb onderzocht welke methode het beste past in de huidige situatie. Dit zijn de drie methodes in kwestie:

- Host-to-host VPN
- Host-to-site VPN
- Site-to-site VPN

Host-to-host

Host-to-host wil zeggen dat er een VPN-verbinding wordt gemaakt tussen twee computers via het Internet. Op de ene computer is VPN client software geïnstalleerd en fungeert als de client, op de ander wordt VPN server software geïnstalleerd en fungeert als de server. Figuur 4-1 op de volgende pagina laat hier een voorbeeld van zien. De client zet de verbinding op en de server handelt de verbinding af. Een VPN server kan meerdere clients afhandelen. Welke VPN client –en server software er nodig is, ligt aan het type VPN-verbinding die gebruikt wordt.

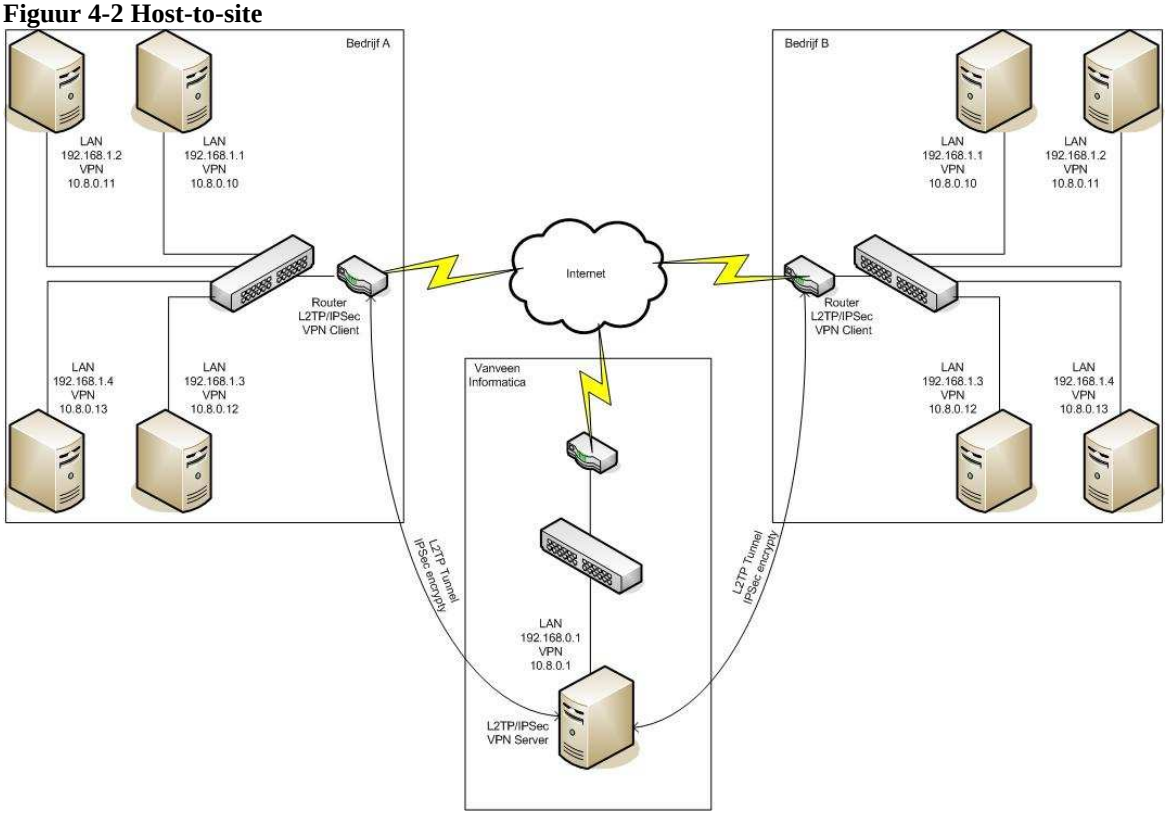
Figuur 4-1 host-to-host



Host-to-site

Host-to-site wil zeggen dat er een VPN-verbinding wordt gemaakt tussen bijvoorbeeld een router en een server. Op deze manier kunnen de routers verbinding maken met de VPN server en is er geen client installatie nodig op de server. Bij een goede configuratie ontstaat een transparant netwerk dat over meer dan een locatie gespreid kan zijn. Tekening 4-2 laat een voorbeeld zien van een host-to-site verbinding.

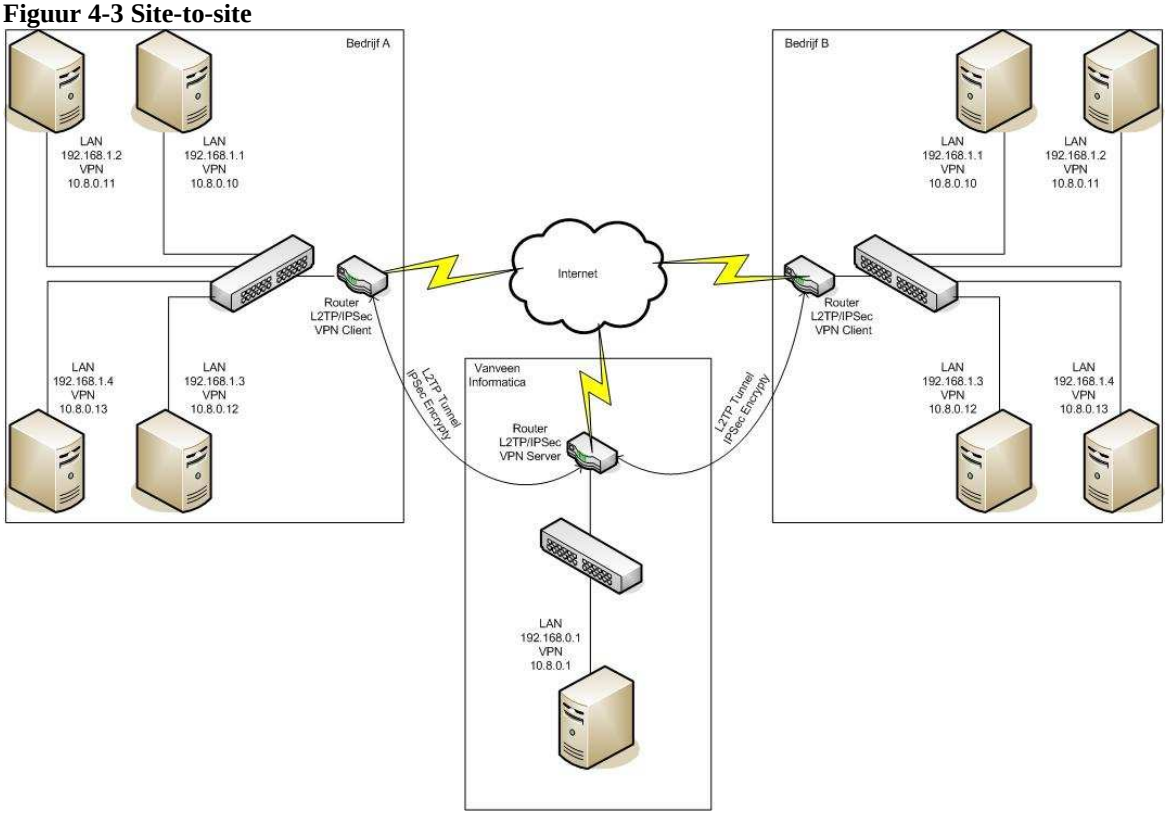
Figuur 4-2 Host-to-site



Site-to-site

Een andere optie is de VPN-verbinding niet te laten maken door de individuele computers, maar bijvoorbeeld door routers te laten afhandelen. Tekening 4-3laat een voorbeeld zien van een site-to-site verbinding. De verschillende servers hoeven in dit geval geen aparte VPN software te gebruiken. Bij een goede configuratie ontstaat een transparant netwerk dat over meer dan een locatie gespreid kan zijn. De firewall in de router schermt tegelijkertijd het hele netwerk achter de router af.

Figuur 4-3 Site-to-site



Uit de klanteninventarisatie in de definitiefase is gebleken dat niet elk bedrijf een router of firewall heeft die een VPN-verbinding ondersteund. Dit betekent dat wanneer er gebruik wordt gemaakt van een site-to-site of host-to-site connectie, dat de bedrijven die geen router hebben met VPN ondersteuning, een router dienen aan te schaffen die wel VPN ondersteunen.

Met een host-to-host connectie wordt er gebruik gemaakt van computers die een VPN-verbinding tot stand brengen in plaats van router of firewall. In de huidige situatie heeft elk bedrijf minimaal één server waarmee VPN-verbinding tot stand kan worden gebracht. Dit betekent dat er minder verandering plaats vind aan de huidige situatie met een host-to-host connectie dan in vergelijking met een site-to-site of host-to-host connectie. Aangezien een wens van de opdrachtgever is dat er geen hardware

wijzigingen mogen plaats vinden in de huidige situatie, heb ik gekozen voor een host-to-host connectie.

4.2 Keuze VPN-verbindingen

In het vorige hoofdstuk is gebleken dat een host-to-host connectie de beste methode is om de virtuele omgeving te verwezenlijken. Hierdoor heb ik op internet verder onderzocht of de vier VPN-verbindingen die in de definitiefase zijn onderzocht een host-to-host connectie konden realiseren. Omdat er per klant, alle servers gemonitored moeten worden, dient erbij dit onderzoek ook rekening gehouden te worden dat er bij een klant meerdere servers kunnen staan. Dit betekent dat alle servers bij een klant een VPN-verbinding dienen op te kunnen opzetten.

In de definitiefase is al gebleken uit mijn onderzoek naar de type VPN-verbindingen en gebruikte technieken dat IPSec achterhaald is. IPSec is vooral bedoeld voor het beschermen van het verkeer tussen diverse netwerken, wanneer dit verkeer via een tussenliggend, niet vertrouwd netwerk ligt. Daarom heb ik deze niet verder onderzocht als VPN-verbinding, het wordt wel gebruikt bij het beveiligingen van L2TP.

De vier VPN-verbindingen die zijn onderzocht of deze een host-to-host connectie konden realiseren zijn:

- MPLS
- L2TP/IPSec
- PPTP
- OpenVPN

Het resultaat van dit onderzoek is dat een MPLS verbinding is uitgesloten omdat dit een VPN-verbinding is die alleen te realiseren is met routers en niet met VPN software. Bij een host-to-host connectie dient er VPN software op de servers geïnstalleerd te worden en daarmee wordt de VPN-verbinding tot stand gebracht. Hierdoor kan er met MPLS geen host-to-host connectie verwezenlijkt worden.

Met PPTP en L2TP/IPSec is het niet mogelijk om een host-to-host connectie te realiseren als er meerdere clients in hetzelfde netwerk bevinden. Dit komt omdat alle klanten gebruiken maken van een router met NAT-functionaliteit om één internetadres te delen tussen alle computers op een netwerk. PPTP en L2TP/IPSec verbreken de verbinding die via een NAT loopt omdat de NAT-adrestoewijzing wordt gezien als een wijziging van het pakket.

Op de site van OpenVPN heb ik kunnen achterhalen dat OpenVPN ook niet de mogelijkheid heeft om met meerdere clients in hetzelfde netwerk een VPN verbinding te maken naar de OpenVPN server. Het is wel mogelijk om één client te verbinden naar een server, maar niet met meerdere clients. Tijdens het onderzoeken hoe een host-to-host connectie gerealiseerd kan worden met OpenVPN, ben ik op het forum

http://gathering.tweakers.net belandt. Op het forum kunnen door leden van de site (gratis registratie) technische vragen gesteld over een bepaald probleem en hier kunnen diezelfde leden ook een reacties op deze vragen plaatsen. Deze reacties zijn niet honderd procent betrouwbaar, omdat iedereen hierop kan reageren, ook mensen met een gebrek aan kennis, maar over het algemeen is te zien aan de uitleg en de beargumentering dat de informatie betrouwbaar is. Op dit forum van heb kunnen achter halen, dat dit opgelost kan worden door een route toe te voegen in het routetabel op de servers achter de OpenVPN client en die als gateway te gebruiken. Op de OpenVPN client dient wel IP forward op 1 te worden gezet in het register, anders kan de OpenVPN client niet de anders computer door routeren naar het virtuele netwerk.

Omdat er ook een alternatieve oplossing gekozen dient te worden en OpenVPN de enige is die een host-to-host connectie kon realiseren, heb ik een keuze gemaakt tussen de andere twee methoden. Deze keuze is gevallen op een site-to-site connectie, omdat er bij een site-to-host aan de host kant dezelfde problemen optreden als bij een host-to-host connectie.
Nu deze methode is gekozen, dient er een keuze gemaakt te worden welke van de VPN-verbindingen het beste een site-to-site connectie kan realiseren met het oog op de huidige situatie. In de klanten inventarisatie die ik in het oriënterend onderzoeksrapport heb opgesteld, staan alle routers die bij de klanten aanwezig zijn. Van de routers die al VPN ondersteunen heb ik gecontroleerd welke VPN's deze ondersteunen. Hieruit is gebleken dat deze routers ondersteuning bieden aan L2TP/IPSec en PPTP, maar niet aan MPLS. Dit betekent dat als MPLS gebruikt wordt, alle routers vervangen moeten worden met routers die MPLS ondersteunen. Dit betekent dat er meer veranderd aan de huidige situatie, dan wanneer er gebruik wordt gemaakt van L2TP/IPSec of PPTP. Aangezien een wens van de opdrachtgever is dat er minimale veranderingen mogen plaats vinden aan de huidige situatie is MPLS afgevallen.

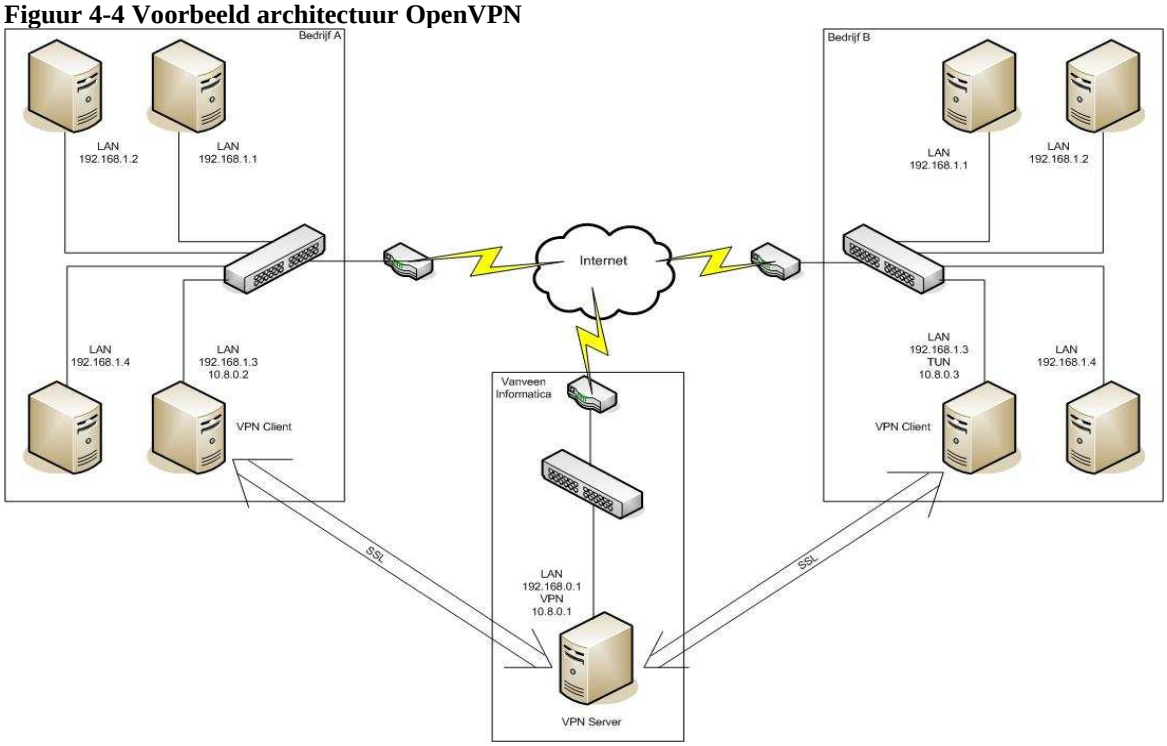
Vervolgens moest er alleen nog een keuze gemaakt worden tussen L2TP/IPSec en PPTP. De keuze tussen deze twee is gebaseerd op de beveiliging, omdat de beveiliging onderzocht is door mijn collega en die heeft geconstateerd dat de beveiliging van PPTP en MPLS onvoldoende zijn. De beveiliging van L2TP/IPSec voldeed wel, hierdoor is alternatieve keuze gevallen op L2TP/IPSec. Hierdoor heb ik niet verder te hoeven onderzoeken met welke van de twee VPN's de virtuele omgeving het beste gerealiseerd kan worden.

Mijn voorkeur is uitgegaan naar OpenVPN, omdat dit gebaseerd is op een host-to-host verbinding en hierdoor hoeft er geen verandering plaats te vinden aan de huidige situatie. Met L2TP/IPSec dient er wel hardware aangeschaft te worden, omdat deze keuze gerealiseerd moet worden met een site-to-site connectie.

Uitwerken van de voorkeursoplossing
Nu de voorkeursoplossing bekend is kan deze verder worden uitgewerkt, door te onderzoeken welke handeling er moeten gebeuren om met OpenVPN een virtuele

omgeving te realiseren. De uitleg die ik hier onder beschreven heb, heb ik kunnen vinden op de website van OpenVPN (www.openvpn.net). Om dit goed te kunnen uitleggen heb ik een tekening gemaakt van een voorbeeld van de nieuwe TI-situatie die te zien is op Figuur 4-4.

Figuur 4-4 Voorbeeld architectuur OpenVPN



In de huidige situatie zijn er meerdere bedrijfsnetwerken, maar voor dit voorbeeld heb ik gebruik gemaakt van de volgende drie netwerken:

- Bedrijf A
- Bedrijf B
- Vanveen informatica

Bedrijf A, bedrijf B en Vanveen informatica hebben allemaal een internet verbinding. De bedrijven A en B hebben beide vier servers in het netwerk staan. In de huidige situatie zijn er bedrijven die meer of minder dan vier servers hebben, maar voor dit voorbeeld heb ik gekozen voor vier servers. Bij Vanveen informatica is er voor de duidelijkheid maar één server opgesteld, omdat de rest van het netwerk geen invloed heeft op de situatie. Deze server fungeert als OpenVPN server.

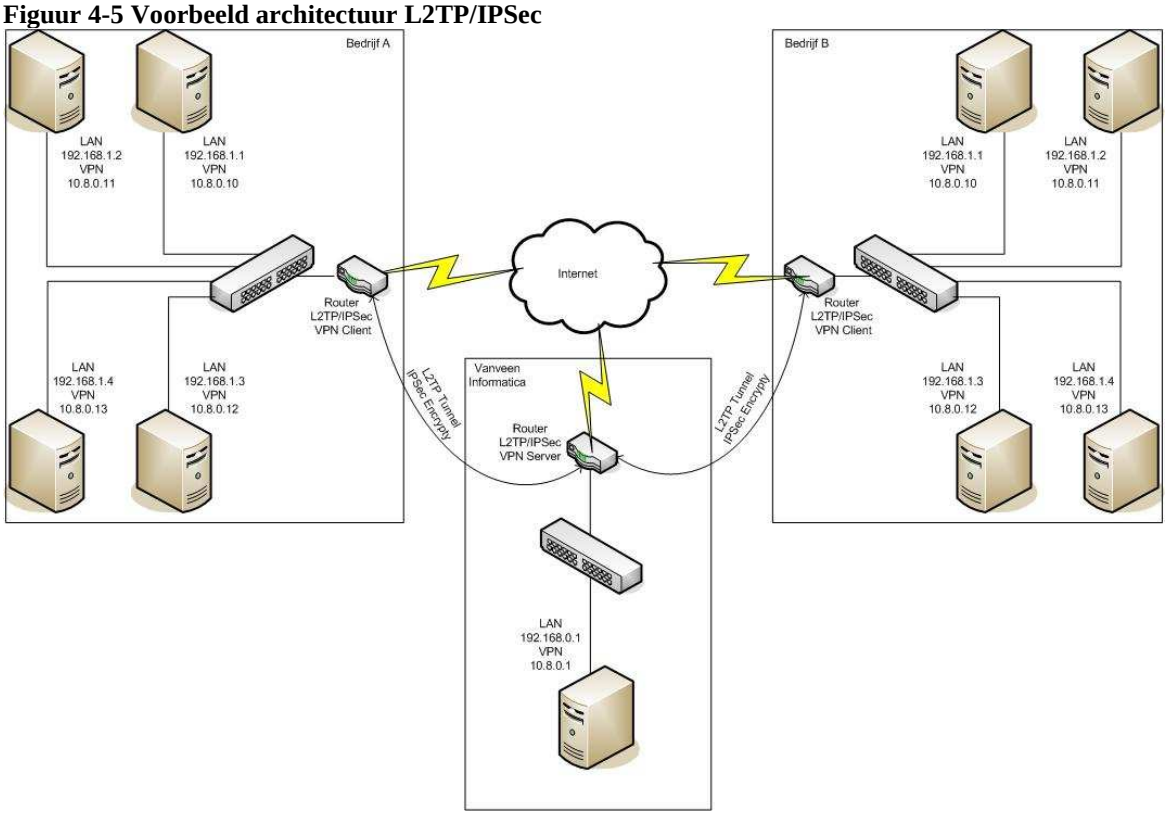
Bij elk bedrijf dient er op één server OpenVPN client software geïnstalleerd en geconfigureerd te worden. Het is niet mogelijk om met meerdere clients verbinding te maken naar de OpenVPN server. Elk bedrijf heeft dus één client die verbinding maakt met de OpenVPN server.

De verbinding wordt tot stand gebracht met een virtuele netwerkkaart, die door de OpenVPN software wordt geïnstalleerd. Deze netwerkkaart kent twee drivers waaruit gekozen kan worden namelijk: TUN en TAP. Op de homesite van OpenVPN heb ik alleen kunnen vinden dat TUN een routed tunnel creëert en TAP een ethernet of bridged tunnel creëert, verder heb ik hier niet over gevonden. Omdat de computers achter de OpenVPN client naar het virtuele netwerk gerouteerd dienen te worden, heb ik gekozen om TUN te gebruiken. Zoals ik al eerder heb beschreven, dienen de andere servers in het netwerk gerouteerd te worden naar het virtuele netwerk, door een route toe te voegen in hun eigen routetabel.

Uitwerken van de voorkeursoplossing L2TP/IPSec

In de tekening hieronder is een voorbeeld gegeven van een site-to-site connectie met L2TP/IPSec. Hierbij geldt net als het voorbeeld bij OpenVPN dat er vier servers staan bij de bedrijfsnetwerken en één server bij Vanveen informatica en hebben ze allemaal een internetverbinding. Alleen in dit geval wordt de verbinding niet tot stand gebracht door een server, maar door een router. De router bij Vanveen fungeert als VPN server en handelt de clients af. De routers bij de bedrijven fungeren als client en maken verbinding met de VPN server bij Vanveen. Ook zorgen de routers ervoor dat het hele netwerk zichtbaar is voor Vanveen en de bedrijven onderling.

Figuur 4-5 Voorbeeld architectuur L2TP/IPSec



4.3 Systeem monitoring software

Hier wordt besproken welke keuzes zijn gemaakt van de in de definitiefase onderzochte monitoring tools. Ook wordt ook uitgelegd waar die keuzes op gebaseerd zijn. Daarna wordt uitgelegd hoe deze keuzes gebruikt kunnen worden in de huidige situatie.

4.3.1 Keuzes voor systeem monitoring software

De monitoring tools die in de definitiefase zijn onderzocht, worden met elkaar vergeleken, met behulp van een matrix. Zie tabel 4.1.

Ook hierbij geldt dat er een voorkeur en alternatieve keuze wordt gemaakt. Bij het beoordelen van de software bleek dat de website van de monitoring tools in kwestie een voldoende bron van informatie is, om de kwaliteiten van het pakket te beoordelen. Er zijn altijd screenshots van de diverse onderdelen van de pakketten getoond en zijn er documenten aanwezig met uitgebreide beschrijvingen.

In tabel 4-1 staat welke waardering een monitoring tool heeft gehad voor een bepaalde kenmerk. Deze kenmerken zijn eisen van de opdrachtgever waar de monitoring tool aan moet voldoen, of kenmerken die een extra toegevoegde waarde brengen aan het product.

Uitleg tekens:

- De plustekens geven aan welke indruk ik kreeg van het kenmerk van een bepaalde monitoring tool.
- Bij een minteken wordt het kenmerk niet ondersteund
- Het sterretje geeft aan dat het standaard niet inbegrepen zit, maar dat het wel gedownload of zelf gemaakt kan worden.

Op deze manier heb ik kunnen aantonen wat de sterke of zwakke punten zijn van een monitoring tool en wordt als hulpstuk gebruikt bij het bepalen van de keuzes.

Tabel 4-1 Matrix van monitoring tools

	Big Brother	Big Sister	Nagios	Zabbix	MOM	MonitorMagic
Windows server installatie	++	+	-	-	+++	+++
Windows client installatie	+++	++	-	-	+++	+++
Linux server installatie	+++	++	++	++	-	-
Linux client installatie	+++	++	++	++	-	-
Configuratie	+++	++	++	++	+	+
Netwerkbeschikbaarheid monitoren	+++	+++	++	++	+++	++
Hardware op een Windows platform monitoren	++	++	++	++	+++	++
Hardware op een Linux platform monitoren	++	++	++	++	*	*
Windows thresholds monitoren	++	++	*	*	+++	++
Linux thresholds monitoren	++	++	+++	+++	*	*
Probleem notificaties[1]	+++	++	+++	++	+++	++
Overzichtelijkheid[1]	++	++	++	++	+++	+++
Plug-ins (uitbreidbaar)	+++	++	++	++	+++	++
Windows event logs monitoren	++	++	*	*	+++	++
Back-upsoftware logs monitoren	*	*	*	*	*	++
Prijs[1]	++	+++	+++	++	+	++
Support	++	++	++	++	+++	++

1) geen eis van de opdrachtgever

+++ Goed
++ Redelijk
+ Matig
- Niet mogelijk
* Met een plugin wel mogelijk

In de tabel is te zien dat MOM de beste waardering heeft ontvangen. Dit komt omdat in een Windows omgeving vrij wel alles zeer uitgebreid te monitoren is. Het nadeel van MOM is dat het niet op Linux systemen geïnstalleerd kan worden, waardoor het Linux besturingsystemen niet optimaal kan monitoren. Met behulp van management packs kan wel het syslog van Linux systemen uitgelezen worden en back-up software logs. Het overzicht waar alle servers op staan is erg duidelijk en de probleem notificaties zijn ook goed geregeld.

MOM is gekozen als alternatief, ondanks de grote hoeveelheid pluspunten. Dit komt omdat de voorkeur is uitgegaan naar Big Brother, wat de meest flexibele monitoring tool is samen met Big Sister. Het zijn de enige tools die op beide platformen geïnstalleerd kunnen worden, wat de schaalbaarheid ten goede komt. Ook het ontwikkelen van een plugin is goed geregeld en heeft het een groot assortiment aan beschikbare plug-ins. Big Sister is ook flexibel, maar levert in op de kwaliteit van de eigenschappen support, probleem notificaties en plugins.

Nagios, Zabbix en MonitorMagic hebben niet de kwaliteit of mogelijkheden die Big Brother en MOM wel hebben, vandaar dat deze niet geselecteerd zijn.

4.3.2 Uitwerken van de voorkeursoplossing

De Big Brother monitoring software bestaat uit server– en client software, die zowel op Linux als Windows te installeren is. Op de OpenVPN server wordt de server software geïnstalleerd en op servers in de virtuele omgeving de client software.

De server software controleert de netwerkbeschikbaarheid van alle servers. Ook kan het allerlei protocollen controleren zoals FTP, HTTP, POP3, SMTP etc. Het heeft het een database waar alle geregistreerde informatie wordt opgeslagen. Met behulp van de webbrowser kan de status van iedere server worden getoond in een overzicht. Als er een probleem is geconstateerd met een of meerdere servers is dat duidelijk zichtbaar in het overzicht of kan ervoor gekozen worden om dit te melden door middel van e-mail of SMS.

Die client software kan alle hardware controleren van de server, maar ook ‘thresholds’ zoals schijfruimte, temperatuur en processor gebruik etc. De geregistreerde gegevens worden naar de server gestuurd en wordt het in een database opgeslagen.

4.3.3 Uitwerken van de alternatieve oplossing

MOM is een enterprise management server en dient op de OpenVPN server geïnstalleerd te worden. Het biedt 1 centrale plek van beheer die wel tot 10000 servers kan beheren en het is een softwarepakket die bijzonder schaalbaar is.

Het is een managementoplossing die werkt met agent of zonder agents. Voor de meeste mogelijkheden installeer je een agent op het te managen systeem. Die agent verzamelt informatie inventariseert die informatie en beoordeelt of hij een sein moet geven aan de management server. Deze agents dienen op de OpenVPN clients geïnstalleerd te worden. Het beheer geef je vorm met regels, deze worden geconfigureerd op de server en worden telkens naar de agent verzonden.

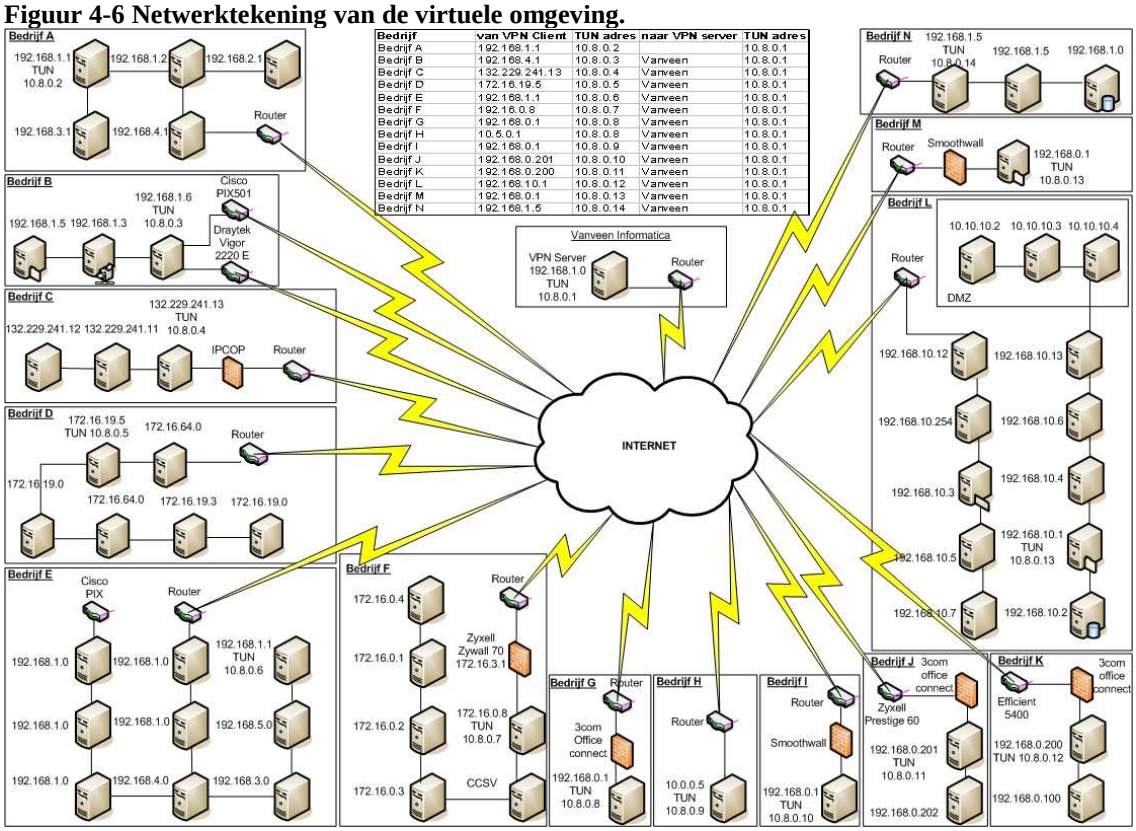
4.4 Netwerktekening

ASI-rapport beschrijft dat er in de architectuurfase een netwerktekening opgesteld dient te worden. Met behulp van de klanten inventarisatie in het oriënterend onderzoeksrapport heb ik een netwerktekening(zie figuur 4.6) kunnen maken, waarop alle servers staan getekend die deelnemen aan de virtuele omgeving. De werkstations van klanten hoeven niet gemonitored te worden, daardoor zijn deze ook niet in de tekening opgenomen. Wel zijn de firewalls en routers opgenomen indien aanwezig bij het bedrijf, omdat hier rekening moet worden gehouden met betrekking tot het openzetten van poorten. Dit komt omdat OpenVPN gebruik maakt van port 1194. Als deze poort geblokkeerd wordt door een firewall, dan wordt het OpenVPN verkeer geblokkeerd.

De voorkeur van de netwerkverbindingen uitgegaan is naar OpenVPN, hierdoor is de tekening gebaseerd op host-to-host OpenVPN-verbindingen. In de tekening is ook een tabel opgesteld, waarin staat welke server in het netwerk een OpenVPN client is en verbinding maakt met de server bij Vanveen informatica. Dit is ook te ze zien aan het TUN IP-adres, het IP-adres van de virtuele netwerkkaart. De privé IP-adressen zijn ook genoteerd van de servers om te kunnen constateren welke privé adressen er gebruikt zijn om te zien in welke range de TUN IP-adressen niet gebruikt mogen worden. Ik heb uiteindelijk gekozen voor de 10.8.0.0 reeks, omdat deze standaard ook gebruikt wordt door OpenVPN en niet voorkomt in andere netwerken.

De namen van de bedrijven en computernamen zijn weggelaten in verband met vertrouwelijke informatie, in plaats daarvan is het aangegeven met Bedrijf A t/m N.

Figuur 4-6 Netwerktekening van de virtuele omgeving.



Bedrijf	van VPN Client	TUN adres	naar VPN server	TUN adres
Bedrijf A	192.168.1.1	10.8.0.2		10.8.0.1
Bedrijf B	192.168.4.1	10.8.0.3	Vanveen	10.8.0.1
Bedrijf C	132.229.241.13	10.8.0.4	Vanveen	10.8.0.1
Bedrijf D	172.16.19.5	10.8.0.5	Vanveen	10.8.0.1
Bedrijf E	192.168.1.1	10.8.0.6	Vanveen	10.8.0.1
Bedrijf F	192.16.0.8	10.8.0.7	Vanveen	10.8.0.1
Bedrijf G	192.168.0.1	10.8.0.8	Vanveen	10.8.0.1
Bedrijf H	10.5.0.1	10.8.0.8	Vanveen	10.8.0.1
Bedrijf I	192.168.0.1	10.8.0.9	Vanveen	10.8.0.1
Bedrijf J	192.168.0.201	10.8.0.10	Vanveen	10.8.0.1
Bedrijf K	192.168.0.200	10.8.0.11	Vanveen	10.8.0.1
Bedrijf L	192.168.10.1	10.8.0.12	Vanveen	10.8.0.1
Bedrijf M	192.168.0.1	10.8.0.13	Vanveen	10.8.0.1
Bedrijf N	192.168.1.5	10.8.0.14	Vanveen	10.8.0.1

5 Ontwerpfase

In deze fase zal er een testplan worden opgesteld. Het testplan is oorspronkelijk een activiteit binnen de ontwikkelfase, maar omdat de ontwikkelfase buiten beschouwing is gelaten en het testen een essentieel onderdeel is van het project, is deze activiteit opgenomen in de ontwerpfase. Het is essentieel omdat er geconstateerd dient te worden of het onderzoek ook daadwerkelijk de gewenste resultaten oplevert.

Verder heb ik een ontwerpdocument opgesteld waarin de configuraties, van OpenVPN en Big Brother beschreven staan. Deze configuraties zijn belangrijk voor de opdrachtgever voor als het ontwerp wordt geïmplementeerd. De testplan is als bijlage toegevoegd aan het ontwerpdocument.

Als laatste is het adviesrapport opgesteld, waarin ik adviseer met welk product een virtuele omgeving gerealiseerd kan worden en met welk product deze omgeving gemonitored kan worden.

5.1 Testplan

Het testplan bestaat uit het testen van OpenVPN en het testen van Big Brother. Met het testplan zou moeten blijken of het onderzoek naar het realiseren van een virtuele omgeving met OpenVPN en het monitoren daar binnen voldoet, conform de eisen van de opdrachtgever.

5.1.1 Testen van een OpenVPN-verbinding

Als eerste heb ik een OpenVPN-verbinding getest tussen twee Windows XP computers. Ik heb hier voor gekozen, omdat ik heel weinig ervaring had met Linux, daardoor is het met Windows voor mij sneller te realiseren.

De twee Windows computers om dit te testen waren mijn laptop en mijn desktop pc. Op mijn laptop heb ik OpenVPN server software geïnstalleerd en op mijn desktop pc OpenVPN client software. Hiermee kan er een OpenVPN-verbinding gerealiseerd worden tussen twee systemen. Ik heb gekozen voor deze kleine opstelling om eerst OpenVPN in de praktijk te ervaren om vervolgens de testopstelling uit te breiden. Dit komt omdat OpenVPN de eerste keer niet eenvoudig te configureren is, want het heeft geen grafische interface en alle configuratie bestanden dienen handmatig aangepast te worden.

Tijdens het installeren van de OpenVPN software op mijn laptop, zijn er een aantal bestanden gekopieerd naar een door mij zelf toegewezen directory op de harde schijf. De bestanden bestaan o.a. uit het server configuratiebestand en scripts die nodig zijn voor het configureren van de OpenVPN server. Met deze scripts worden certificaten en sleutels gegenereerd. Dit is verder voor mij niet relevant, maar wel voor mijn medestudent, want dit is onderdeel van de beveiliging.

Ook wordt tijdens de installatie een virtuele netwerkkaart geïnstalleerd. Dit is een virtuele netwerkkaart die gebruik wordt voor de VPN-verbinding en deze verbinding kan in twee mogelijkheden worden gecreëerd. Het verschil zal ik bij het client configuratiebestand uitleggen.

Voor het configureren van de server wordt het server configuratiebestand aangepast. Het bestand ziet er als volgt uit:

Figuur 5-1 OpenVPN server configuratiebestand

server.ovpn - Kladblok

Bestand Bewerken Opmaak Beeld Help

```
port 1194 #hiermee kan een poort aangewezen worden aan OpenVPN,
          standaard gebruikt het 1194.

proto udp #hiermee geef je aan dat je een udp of TCP/IP connection wilt.
          udp is connectionless, dit zorgt voor minder vertraging.

;dev tap
dev tun
#Er kan gekozen wordt tussen een tap of tun virtuele netwerkkaart.

ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\config\\server.crt"
key "C:\\Program Files\\OpenVPN\\config\\server.key"
dh "C:\\Program Files\\OpenVPN\\config\\dh1024.pem"
# Dit zijn de certificaten, sleutels en encrypties.
De ca.crt en dh1024.pem wordt ook door de OpenVPN clients gebruikt.


server 10.8.0.0 255.255.255.0 #het virtuele ip-adres + subnetmask van de server


route 192.168.0.0 255.255.255.0 #het adres van de clients


keepalive 10 120 # Als er geen connectie meer is met een bepaalde client,
                 pingt hij elke 10 sec gedurende 120 sec om te
                 controleren of de client wel echt down is



comp-lzo        #zorgt ervoor dat de datacompressie aanstaat


persist-key
persist-tun
#Deze 2 zorgen ervoor dat als er rechten zijn veranderd, dat na de restart,
       ze geen toegang meer tot de rechten die veranderd zijn.


status openvpn-status.log #Dit zorgt ervoor dat alle statusgegevens opgeslagen
                          wordt naar dat bestand


verb 3 # dit geeft de mate aan, op hoeveel punten er gelogd moet worden.
```

Waar deze regels voor dienen heb ik uitgezocht op de website van OpenVPN en in het originele server configuratiebestand staat ook uitleg gegeven waar het voor dient. Ik heb ook commentaar toegevoegd om aan te geven wat de regels voor functie hebben.

In het configuratiebestand staat beschreven dat er gekozen kan worden tussen TUN en TAP. In het vorige hoofdstuk had ik al beschreven, dat ik niet duidelijk kon vinden wat het echte verschil is, maar door dit verder onderzocht te hebben op internet werd het mij duidelijker. TUN driver creëert een routed tunnel en maakt gebruik van IP frames en een TAP driver een creëert ethernet tunnel en maakt gebruik van ethernet frames.

Vervolgens heb ik OpenVPN client geïnstalleerd. Deze wordt op dezelfde manier geïnstalleerd als de server, alleen moet dit keer het client configuratiebestand aangepast worden. Het bestand ziet er als volgt uit:

Figuur 5-2 OpenVPN client configuratiebestand

client.ovpn - Kladblok

Bestand Bewerken Opmaak Beeld Help

```
client #om aan te geven dat het de client is

;dev tap
dev tun #ook hier kan gekozen worden tussen tun of tab

proto udp #


remote 192.168.0.1 1194 #Het IP-adres van de OpenVPN server


resolv-retry infinite #Als er geen verbinding is met de server blijft
                      reconnecten tot er weer verbinding is.

nobind # hiermee zet je de mogelijk uit om een specifieke
port toe te wijzen aan een lokale port

persist-key
persist-tun
#Deze 2 zorgen ervoor dat als er rechten zijn veranderd, dat na de restart,
        ze geen toegang meer tot de rechten die veranderd zijn.

ca "C://Program Files//OpenVPN//easy-rsa//keys//ca.crt"
cert "C://Program Files//OpenVPN//easy-rsa//keys//client1.crt"
key "C://Program Files//OpenVPN//easy-rsa//keys//client1.key"
dh "C://Program Files//OpenVPN//easy-rsa//keys//dh1024.pem"
#Certificaten en sleutels en encrypties. deze client1.crt en
client.key dienen op de server aangemaakt te worden. ca.crt en
dh1024.crt zijn de dezelfde als die van de server.

ns-cert-type server
# Dit geeft aan dat je de certificaat van de server gebruikt

comp-lzo #Zorgt ervoor dat de compressie aanstaat

verb 3 # dit geeft de mate aan, op hoeveel punten er gelogd
moet worden.
```

De client configuratiebestand in figuur 5-2 ziet er vrijwel hetzelfde uit als het server configuratiebestand in figuur 5-1, alleen zijn er een aantal regels bijgekomen of weggelaten. Het is logisch dat als bijvoorbeeld TUN of UDP gebruikt wordt op de server, dat het dan ook in dit bestand gebruikt wordt.

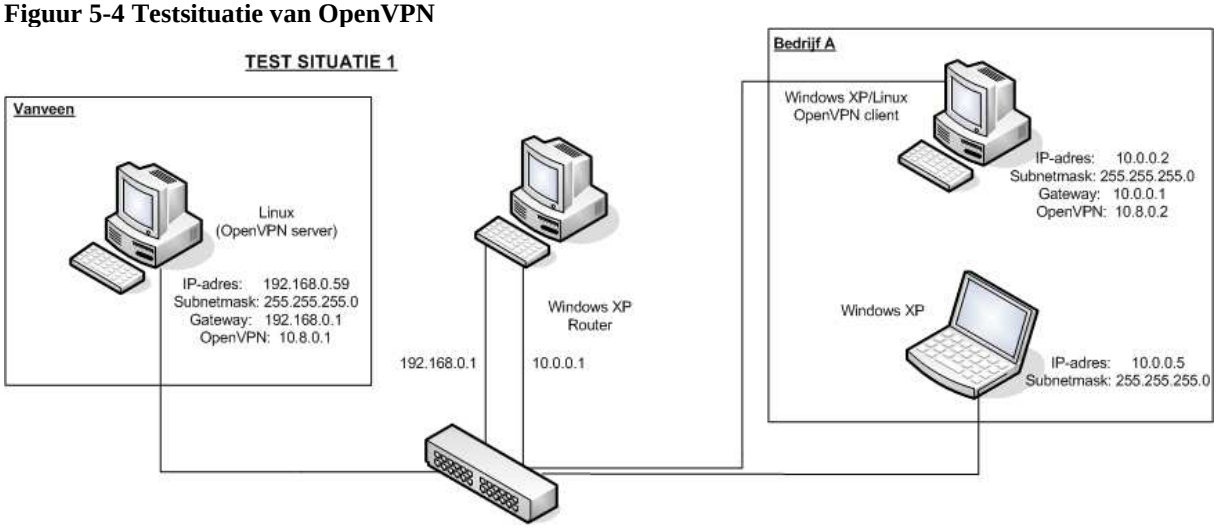
De connectie is getest door een ping te sturen naar het virtuele IP-adres (10.8.0.1) van de OpenVPN server vanaf de client en een ping te versturen van de OpenVPN server naar het virtuele adres van OpenVPN client. In Figuur 5-3 is het resultaat te zien van een ping-test.

Figuur 5-3 Ping-test

5.1.2 Testen van de virtuele omgeving

Vervolgens heb ik getest of een tweede computer in hetzelfde netwerk als de OpenVPN client gebruik kan maken van het virtuele netwerk. Deze test is noodzakelijk omdat ook de servers achter de OpenVPN client gemonitored moeten worden via het virtuele netwerk. Als dit niet mogelijk is dan zal er naar een andere oplossing gezocht moeten worden. Van deze situatie heb ik vervolgens eerst een tekening gemaakt. Zie figuur 5-4 op de volgende bladzijde voor de tekening.

Figuur 5-4 Testsituatie van OpenVPN



Voor het installeren van OpenVPN heb ik dit keer een Linux desktop pc gebruikt als OpenVPN server. De opdrachtgever had na het lezen van het architectuurdocument aangegeven dat hij de voorkeur gaf aan een Linux server met OpenVPN server software. Het installeren van het Linux besturingsysteem ging mij wel goed af, maar het installeren van OpenVPN ging een stuk moeizamer. Dit kwam door mijn beperkte kennis van Linux, maar met behulp van handleidingen die ik op internet gevonden heb, is het mij wel gelukt om Linux te installeren.

Om dit te kunnen te testen had ik minimaal 3 computers en een router nodig. Zelf had ik een laptop en een werkstation, dus kwam ik twee pc's te kort. Vervolgens heb ik dit aangegeven bij de opdrachtgever die met een aantal pc's te voorschijn is gekomen, waar ik vervolgens de tekening mee heb na kunnen bootsen. De situatie bestaat uit een het volgende:

- Een Linux CentOS desktop pc, waarop OpenVPN server software geïnstalleerd is
- Een Windows XP desktop pc met twee netwerkkaarten die als router fungeert
- Een Windows XP desktop pc met OpenVPN client software
- Een Windows XP laptop

Mijn laptop is het tweede systeem in het netwerk, die naar het virtuele netwerk gerouteerd wordt zodra er een route is toegevoegd. Dit is een route van het LAN IP-adres van de laptop, via het virtuele adres van de OpenVPN client, naar het virtuele adres van de OpenVPN server. Op de OpenVPN client dient wel IP forward op 1 te worden gezet in het register, zodat het de andere computers kan routeren naar het virtuele netwerk. De Linux OpenVPN server bevindt zich in een ander netwerk dan de twee systemen in bedrijf A. De router is ingezet zodat er toch een route is naar beide netwerken. Hiervoor dient dan wel de router als gateway ingesteld te worden op de OpenVPN server en OpenVPN client. Belangrijk hierbij is dat er geen gateway wordt ingesteld op de laptop, want hierdoor is het niet mogelijk voor de laptop, om bij de OpenVPN server te komen via het normale netwerk. Hierdoor is het mogelijk om te

testen of hij naar het virtuele netwerk gerouteerd kan worden zonder gebruik te maken van het normale netwerk.

Als eerste heb ik getest of de computers onderling met elkaar kunnen communiceren, zonder daarbij routes toe te voegen. Dit heb ik gedaan om zeker te weten dat er geen route is van de laptop naar de server en andersom. Met deze test verwacht ik het volgende:

- De OpenVPN server kan de OpenVPN client pingen en andersom.
- De laptop in bedrijf A kan de OpenVPN server niet pingen, omdat er geen route is toegevoegd naar het virtuele netwerk.
- De OpenVPN server kan de laptop in bedrijf A niet pingen

Het resultaat is terug zien in het onderstaande tabel.

Tabel 5-1 Testsituatie 1

Systeem	OpenVPN server	OpenVPN client	Laptop
OpenVPN server		√	X
OpenVPN client	√		√
Laptop	√	√	

Door deze test heb ik twee problemen geconstateerd. Het eerste probleem is dat de laptop een route heeft naar het virtuele netwerk, zonder dat er een route is toegevoegd in het route tabel. Vervolgens heb ik het routetabel bekeken en constateerde ik dat er een route naar het virtuele netwerk is toegevoegd. Dit betekent dat iedere PC in het lokale netwerk die zich achter de OpenVPN client bevindt automatisch een route krijgt toegevoegd. Dit leek voor mij in eerst instantie geen probleem, omdat er een route is naar het virtuele netwerk, ook al is de route niet handmatig ingevoerd. Toen mijn collega aangaf dat dit consequenties heeft voor de beveiliging, is het wel mijn probleem geworden en heb ik hier een oplossing voor moeten vinden. Het twee probleem is dat de OpenVPN server niet kan pingen naar de laptop. Dit is logisch omdat er geen route is, maar ik realiseerde dat als er een route wordt gemaakt dat dit een route is naar een LAN IP-adres. Dit komt omdat de laptop geen virtueel IP-adres heeft, maar een LAN IP-adres. Daarna realiseerde ik dat er klanten zijn die dezelfde IP-adressen gebruiken, want dit zijn privé IP-adressen waar iedereen gebruik van mag maken. Dit betekent dat de OpenVPN server, routes dient te maken naar IP-adressen die meerdere keren voorkomen en dat is niet mogelijk. Deze route is wellicht noodzakelijk als de monitoring tool de beschikbaarheid van de clients wil monitoren. Deze

Vervolgens heb ik naar een oplossing gezocht van het eerste probleem op het internet. De oplossing die ik gevonden heb is het gebruik maken van een TAP driver in plaats van een TUN driver. Eerder had ik al gevonden dat een TUN driver een routed tunnel creëert en gebruik maakt van IP frames en een TAP driver een ethernet tunnel creëert en maakt gebruik van ethernet frames. Dit betekent dat TUN met laag 1, 2 en 3 werkt van het OSI-model en TAP werkt alleen met laag 1 en 2 van het OSI-model. Omdat

TUN ook gebruik maakt van laag 3 kan het IP pakketjes versturen naar computers achter de OpenVPN client, zodat ook deze computers gebruik kunnen maken van het virtuele netwerk. De oplossing heb ik getest door de configuratie bestanden van de server en client te wijzigen, zodat er verbinding wordt opgezet met een TAP driver in plaats van een TUN.

Met deze test verwacht ik het volgende:

- De OpenVPN server kan de OpenVPN client pingen en andersom.
- De laptop kan de OpenVPN server niet pingen, omdat er geen route is toegevoegd naar het virtuele netwerk.
- De OpenVPN server kan de laptop in bedrijf A niet pingen

Het resultaat is te zien in de onderstaande tabel.

Tabel 5-2 Testsituatie 2

Systeem	OpenVPN server	OpenVPN client	Laptop
OpenVPN server		√	X
OpenVPN client	√		√
Laptop	X	√	

Hieruit blijkt dat de laptop de OpenVPN server niet kan pingen zonder een route toegevoegd te hebben. Vervolgens kan er getest worden of de OpenVPN client de OpenVPN server kan pingen, door de route toe te voegen in de route tabel.

Met deze test verwacht ik het volgende:

- De laptop kan de OpenVPN server pingen.

Het resultaat is te zien in het onderstaande tabel.

Tabel 5-3 Testsituatie 3

Systeem	OpenVPN server
OpenVPN server	
Laptop	√

Uit het tabel blijkt dat de oplossing voor het eerste probleem is gevonden, maar dient er nog een oplossing gevonden te worden voor het tweede probleem.

Bij het bedenken voor een oplossing van het tweede probleem realiseerde ik dat dit opgelost kon worden met Big Brother. In het oriënterend onderzoeksrapport had ik al de mogelijkheden van Big Brother beschreven en een van deze mogelijkheden is zelf ontwikkelde scripts toevoegen. Omdat de laptop wel de mogelijkheid heeft om gegevens naar de Big Brother server te sturen heeft, dacht ik dat als ik een script zou schrijven die een ping verstuurd naar de server en het resultaat vervolgens doorstuurt

naar de Big Brother server, dat dit de oplossing zou kunnen zijn. Dit dient dan getest te worden bij het testen van Big Brother.

5.1.3 Het installeren van de Big Brother server

Voordat het testen van Big Brother van start kan gaan, dient als eerste de Big Brother server software geïnstalleerd. Deze dient geïnstalleerd te worden op de Linux server, waar ik ook al de OpenVPN server op heb geïnstalleerd, zodat ik daarna kan testen of de OpenVPN clients die verbonden zijn met de OpenVPN server gemonitored kunnen worden door Big Brother.

Zoals ik al in hoofdstuk 4.2.1 heb uitgelegd, controleert de Big Brother server de netwerkbeschikbaarheid van computers en fungeert als centraal punt in het netwerk. De Big Brother client controleert de hardware, services en event logs en verzend zijn gegevens naar de Big Brother server. De benodigdheden voor het installeren van Big Brother server zijn:

- Big Brother server software
- Apache
- PHP

Voordat de Big Brother server geïnstalleerd kan worden dient er als eerste Apache te worden geïnstalleerd. Dit is een webserver die nodig is om Big Brother te gebruiken. Dit heb ik kunnen installeren en configureren doormiddel van een handleiding, die ik op het internet gevonden heb. Uit dezelfde handleiding heb ik PHP kunnen installeren, want ook dit is nodig om Big Brother te kunnen gebruiken. Vervolgens heb ik de Big Brother server software geïnstalleerd, maar dit was voor mij een lastige opgave door mijn gebrek aan kennis van Linux. Met behulp van de handleiding van Big Brother en handleidingen op internet heb ik de Big Brother server kunnen installeren.

Om ook te kunnen testen dat de hardware en log bestanden van de Linux server worden gemonitored, dient de Big Brother client sofware geïnstalleerd te worden. Deze client kan ook naast de Big Brother server geïnstalleerd worden. Hiermee is het gelijk de Big Brother client op Linux getest. De Big Brother client heb ik wel zonder problemen kunnen installeren.

5.1.4 De hostfile van de Big Brother server aanpassen

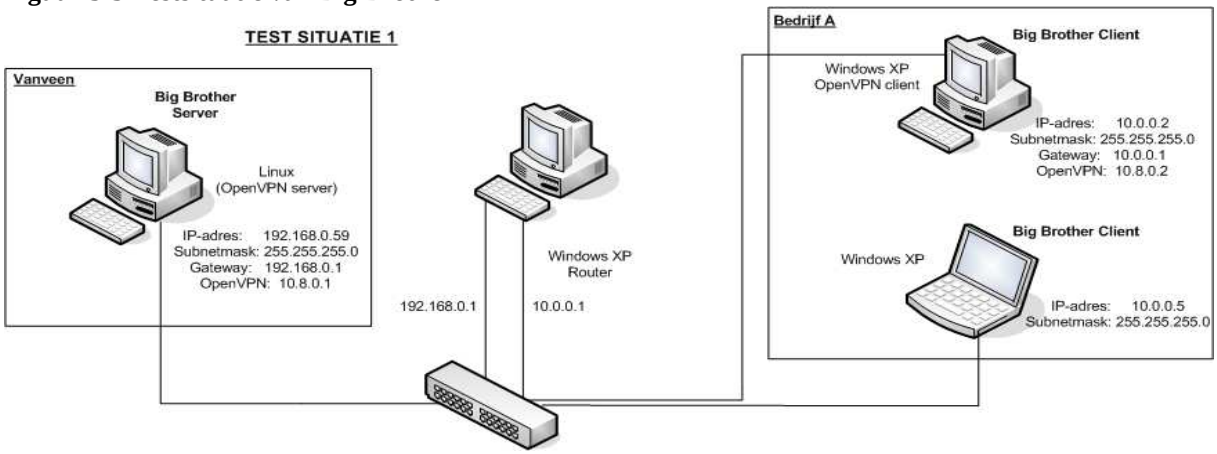
Na het installeren van de Big Brother software dient de Big Brother server nog geconfigureerd te worden, zodat het computers in de virtuele omgeving kan monitoren. In de handleiding van Big Brother heb ik gevonden dat de hostfile van de Big Brother server aangepast dient te worden. Hier kunnen de IP-adressen worden ingevuld van de te monitoren computers en deze worden dan vervolgens door de Big Brother server gemonitored.

5.1.5 Testen binnen de virtuele omgeving met Big Brother

Nu de Big Brother server werkt kan het monitoren binnen de virtuele omgeving getest worden. Tijdens het testen van OpenVPN had ik al een virtuele omgeving gerealiseerd, dus kan het testen van Big Brother in dezelfde opstelling plaats vinden. De tekening heb ik wel aangepast en die is op de volgende bladzijde te vinden.

Daarnaast heb ik ook nog de Big Brother clients op de Windows XP systemen geïnstalleerd, zodat ik kan testen of deze systemen hun informatie naar de Big Brother server sturen via het virtuele netwerk. Met deze informatie bedoel ik dan de hardwaregegevens, log bestanden, thresholds etc.

Figuur 5-5 Testsituatie van Big Brother



Met deze opstelling wil ik het volgende testen:

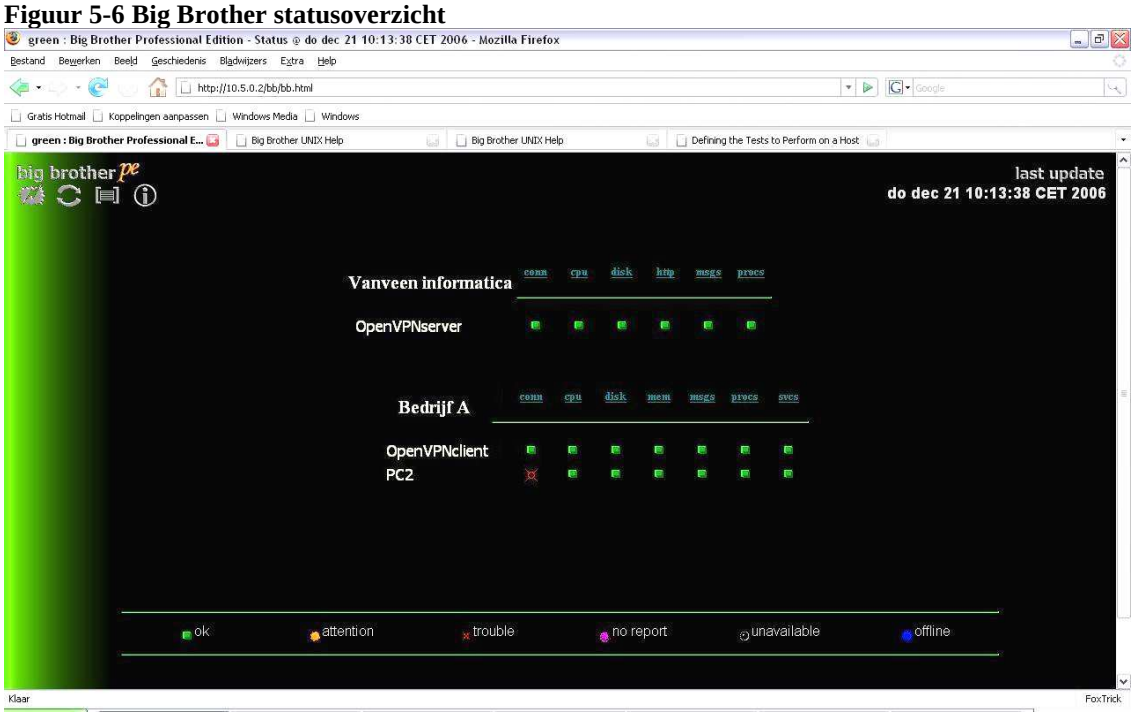
- Testen of beide Big Brother clients hun gegevens verstuurt naar de Big Brother server via het virtuele netwerk.
- Testen of de netwerkbeschikbaarheid van alle systemen worden gemonitored door de Big Brother server.
- Testen of alle servers worden getoond in de webinterface.

Met deze test verwacht ik het volgende:

- De clients versturen hun gegevens naar de server via het virtuele netwerk
- De netwerkbeschikbaarheid van de server en de OpenVPN client worden gemonitored. Het systeem achter de OpenVPN client kan niet worden gemonitored door de server.
- De servers worden allemaal weergegeven in de webinterface.

Het resultaat is te zien in de onderstaande screendump:

Figuur 5-6 Big Brother statusoverzicht



De screendump laat een overzicht zien van alle computers die gemonitored worden in virtuele omgeving. Hier is te zien dat alleen PC2 een fout geeft. Dit is een verwacht resultaat, omdat dit de laptop is achter de OpenVPN client. Verder is er geconstateerd dat clients hun gegevens versturen naar Big Brother server via het virtuele netwerk.

5.1.6 Het creëren van een extern script

Om het probleem op te lossen dat PC2 niet gemonitored kan worden heb ik eerst moeten onderzoek hoe externe scripts worden gecreëerd. Bij het bedenken van de oplossing van dit probleem, realiseerde ik mij dat het wel mogelijk is om te pingen van PC2 naar de Big Brother server. Als ik een script kon maken waarmee de client een ping kan versturen naar de server en vervolgens dit doorgeeft aan de server dan kan dit hiermee worden opgelost.

Met behulp van de Big Brother handleiding heb ik onderzocht hoe deze scripts zelf gecreëerd kunnen worden. Big Brother biedt de mogelijkheid om met externe scripts, zaken te monitoren die standaard niet worden gemonitored door Big Brother.. De scripts kunnen in elke taal geschreven worden, als het script maar uitvoerbaar is door de Big Brother client en een log genereert. Het gegenereerde log bestand mag geen extensie bevatten en de naam van het bestand, is dezelfde naam die getoond wordt in de webinterface.

Het log bestand moet beginnen met “red”, “green” of “yellow”, zodat Big Brother weet welke kleur hij moet tonen in de webinterface. Op deze manier weet Big Brother wat de

status is van de zaken die gemonitored worden. Bijvoorbeeld als er gecontroleerd wordt dat een back-up gelukt is, dient de log te beginnen met “green”, als er geen log gevonden is “red” en bij een fout tijdens de back-up “yellow”. Verder hoeft erin principe geen tekst meer in voor te komen, want dit heeft verder geen effect op Big Brother. De tekst die erna wordt ingevoerd wordt is zichtbaar in het statusrapport als er op het groene, rode, of gele vierkant wordt gedrukt.

5.1.7 Systemen achter de OpenVPN client monitoren

Voor Windows Big Brother clients heb ik dit probleem opgelost door een script te maken met behulp van deze website http://support.bb4.com en de uitleg van de handleiding van Big Brother. In dit script wordt een ping verstuurd naar het IP-adres van de Big Brother server en vervolgens wordt het resultaat opgeslagen in een log bestand. Dit log bestand wordt verstuurd door de Big Brother client naar de Big Brother server en dit resultaat is ook terug te lezen op de webinterface. Hieronder volgt het script.

```
@echo off
:: Batchfile om een andere machine te pingen en het resultaat
versturen naar BB
:: De target PC:
set TARGET=192.168.4.5
:: Deze machine:
set THISMACHINE=192.168.4.2
:: De output waar big brother client het ophaald
set OUTPUTFILE= conn2
:: tempfiles:
set PINGOUTPUT=c:\windows\temp\$ping.tmp
set TMPFILE=c:\windows\temp\$bbping.tmp
:: Het pad naar ping.exe:
set PINGPROG=c:\windows\system32\ping.exe
:: controleer of ping.exe gevonden is.
if not exist %PINGPROG% goto noping
:: echo ping target
%PINGPROG% %TARGET% >> %PINGOUTPUT%
:: controleer of het gelukt is.
if errorlevel ==1 goto bad
goto good
:noping
echo yellow [%THISMACHINE%] %PINGPROG% not found. > %TMPFILE%
goto Continue
:good
echo green [%THISMACHINE%] ping to %TARGET% > %TMPFILE%
goto Continue
:bad
echo red [%THISMACHINE%] ping to %TARGET% failed! > %TMPFILE%
goto Continue
:Continue
echo. >> %TMPFILE%
if exist %PINGOUTPUT% type %PINGOUTPUT% >> %TMPFILE%
copy %TMPFILE% %OUTPUTFILE% > NUL
```

```
:: cleanup
if exist %TMPFILE%  del %TMPFILE%
if exist %PINGOUTPUT% del %PINGOUTPUT%
```

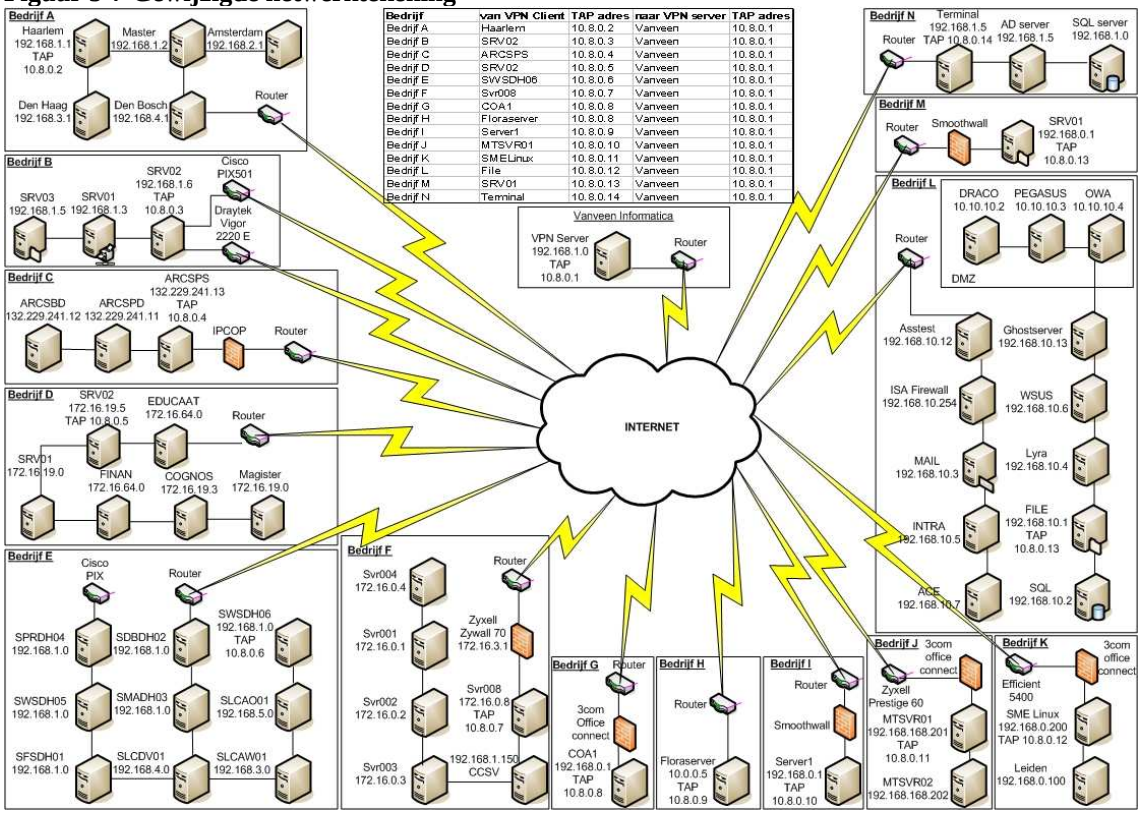
Dit script werkt niet onder Linux, maar ik heb wel een ander script gezien op de user community site Big Brother www.deadcat.net, die dezelfde functie heeft.

5.2 Opstellen ontwerpdocument

In het ontwerpdocument heb ik de configuraties beschreven die gebruikt zijn tijdens het testen. In overleg met de opdrachtgever is besloten om geen handleidingen op te stellen voor de installatie van OpenVPN. Dit komt omdat het schrijven van handleiding meer implementatieniveau is en implementatie valt buiten de scope van het project.

In de bijlage is het testplan opgenomen en de nieuwe netwerktekening. Na het testen van de virtuele omgeving is geconstateerd, dat vorige netwerktekening niet voldoet
In de tekening is de TUN gewijzigd naar TAP en zijn de virtuele IP-adressen gewijzigd.
Tijdens het testen van OpenVPN is gebleken dat het gebruik van de TAP drivers veiliger is dan de virtuele TUN drivers. Dit is terug te lezen in paragraaf 5.1.2.
Mijn collega heeft constateert dat het niet nodig is om elk bedrijf in een aparte range te zetten, om het dataverkeer tussen de bedrijven af te schermen. Hierdoor heb ik ook de IP-ranges gewijzigd.

Figuur 5-7 Gewijzigde netwerktekening



Bedrijf	van VPN Client	TAP adres	naar VPN server	TAP adres
Bedrijf A	Haarlem	10.8.0.2	Vanveen	10.8.0.1
Bedrijf B	SRV02	10.8.0.3	Vanveen	10.8.0.1
Bedrijf C	ARCSPS	10.8.0.4	Vanveen	10.8.0.1
Bedrijf D	SRV02	10.8.0.5	Vanveen	10.8.0.1
Bedrijf E	SWSDH06	10.8.0.6	Vanveen	10.8.0.1
Bedrijf F	Svr008	10.8.0.7	Vanveen	10.8.0.1
Bedrijf G	COA1	10.8.0.8	Vanveen	10.8.0.1
Bedrijf H	Floraserver	10.8.0.8	Vanveen	10.8.0.1
Bedrijf I	Server1	10.8.0.9	Vanveen	10.8.0.1
Bedrijf J	MTSVR01	10.8.0.10	Vanveen	10.8.0.1
Bedrijf K	SMELinux	10.8.0.11	Vanveen	10.8.0.1
Bedrijf L	File	10.8.0.12	Vanveen	10.8.0.1
Bedrijf M	SRV01	10.8.0.13	Vanveen	10.8.0.1
Bedrijf N	Terminal	10.8.0.14	Vanveen	10.8.0.1

5.3 Adviesrapport

In het adviesrapport heb ik beschreven welke producten door mij worden geadviseerd om een virtuele omgeving te realiseren en te monitoren. Ook heb ik beschreven wat de mogelijkheden zijn van de producten.

6 Proces en Productevaluatie

In dit hoofdstuk worden de opgeleverde producten en het gevolgde proces geëvalueerd. Per werkzaamheid en product wordt beschreven welk nut dit gehad heeft.

6.1 Productevaluatie

In dit hoofdstuk worden de geleverde producten geëvalueerd.

Plan van aanpak

Het plan van aanpak is erg belangrijk geweest voor mij, omdat het mij het inzicht heeft gegeven in hoe het project in goede banen geleidt moet worden. In de planning heb ik de fases opgenomen van het ASI-rapport, de methode die ik dit project gehanteerd heb. Hierdoor kon ik de planning gebruiken als leidraad voor de uit te voeren activiteiten.

Het hoofdstuk werkwijze is ook belangrijk voor mij geweest, hier heb ik globaal op papier gezet welke werkwijze ik wilde hanteren om mijn doelstellingen te behalen. Dit heeft mij een beter overzicht gegeven hoe de doelstellingen behaald moesten worden

Oriënterend onderzoeksrapport

Het oriënterend onderzoeksrapport is belangrijk geweest om gevonden informatie terug te vinden. Het terug kijken naar dit document is vaak voorgekomen in de architectuurfase bij het maken van keuzes. Zonder dit document had ik de informatie die ik later nodig had niet zo snel terug kunnen vinden. Ook heb ik mijn kennis uitgebreid door verschillende VPN's en monitoring tools te onderzoeken.

Architectuurdocument

In dit document heb ik een voorkeur en alternatieve keuze gemaakt van elk onderdeel die ik onderzocht heb. Ik vind dat ik de juiste methode heb toegepast en duidelijk heb beschreven hoe ik tot de keuzes ben gekomen. Ook de beschrijving van de architectuur van OpenVPN is goed beschreven, want deze informatie heb ik goed kunnen gebruiken tijdens het testen.

De keuzes zijn voor mij erg lastig gemaakt, omdat ik rekening moest houden met de huidige situatie. Met een router was het ontwerpen van een virtuele omgeving veel eenvoudiger te realiseren geweest en met VPN software is dat een stuk lastiger te realiseren. Hierdoor heb ik veel moeten onderzoeken en tijdens het testen heb ik daar ook problemen mee ondervonden. Ik ben erg tevreden dat ik dit goed heb kunnen oplossen zonder dat daar een concessie bij heeft plaats gevonden. Ook ben ik tevreden van mijn keuze voor de monitoring tool, omdat het voldoet aan de eisen van de opdrachtgever.

Ontwerpdocument
Het testplan dat als bijlage aan dit document is toegevoegd is erg belangrijk geweest. Het testen was essentieel omdat ik dan wist dat het onderzoek ook echt in de praktijk werkte. Ook voor het bedrijf is dit belangrijk, want als in de praktijk bleek dat OpenVPN niet werkte dan moest er terug worden gevallen op een site-to-site connectie. Dit komt omdat hierbij de hardware gewijzigd moet worden en zou er een concessie plaats vinden en dan was het ontwerp minder aantrekkelijk geweest voor de opdrachtgever.

Adviesrapport
Van het adviesrapport heb ik geleerd hoe dit document wordt opgebouwd en wat er in komt te staan. Ik heb duidelijk beschreven wat er mogelijk is met mijn geadviseerde producten.

6.2 Procesevaluatie
In deze paragraaf wordt de evaluatie opgenomen die betrekking heeft op de procesgang van mijn afstudeerperiode.

Ontwikkelmethode
Ik ben erg blij met de keuze van het ASI-rapport. De ontwikkelmethode heeft mij een goed overzicht gegeven hoe het project gefaseerd te werk moest gaan. Een groot voordeel van deze methode is dat er een duidelijke structuur inzit om tot een goed ontwerp te komen.

Planning
Ik heb een realistische planning opgesteld, want ik liep precies op schema en mijn doelstellingen zijn behaald. Ik heb ook een aantal keren de planning gewijzigd, maar dit waren geen drastische veranderingen.

Onderzoek
Het creëren van een virtuele omgeving is iets waar vrij weinig over te vinden is. Ik heb voor het onderzoeken bijna alleen maar gebruik gemaakt van het internet, omdat ik geen boeken tot mijn beschikking had waar deze informatie in stond. Ik vond het soms erg lastig om soms de juiste informatie te vinden op het internet. Veel tijd heb ik doorgebracht op de homepagina van OpenVPN. Deze pagina was erg onoverzichtelijk en het vinden van de juiste informatie was daardoor erg lastig.

Leerpunten
Tijdens mijn afstudeerperiode heb ik veel kennis opgedaan van de verschillende VPN’s. Naast de ervaring die ik opgedaan heb, met het gebruiken van ASI-rapport als ontwikkelmethode, heb ik tijdens deze periode veel kennis verkregen van VPN’s, voornamelijk OpenVPN. OpenVPN heb ik in de praktijk gebruikt, hierdoor is niet alleen mijn theoretische kennis vergroot, maar heb ik daardoor ook praktische kennis vergaard. Verder heb ik mijn theoretische kennis vergroot bij het onderzoeken van de

verschillende VPN technieken die er zijn. Ook heb ik geleerd hoe een virtuele omgeving gerealiseerd kan worden en met welke verschillende methodes en soorten VPN’s dit kan.

Verder heb ik meer inzicht gekregen wat er allemaal mogelijk is met monitoring tools en heb ik mijn kennis en ervaring vergroot van Linux door het installeren en configureren van OpenVPN en Big Brother op een Linux server.

7 Literatuurlijst

Boeken:
Cisco Systems, *CCNP 2: Remote Access Companion Guide 2e editie*

Internetbronnen:
http://www.openvpn.net

http://support.microsoft.com/kb/325034/nl

http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html

http://bb4.net

http://www.zabbix.com

http://nagios.org

http://www.microsoft.com/netherlands/mom/kenmerken.aspx

http://www.tools4ever.com/products/monitormagic/features/application-monitoring/

http://www.bigsister.ch/

http://www.monitorware.com/Common/en/Articles/syslog-described.php

http://www.microsoft.com/technet/prodtechnol/windows2000serv/support/vpnclientag.mspx

http://en.wikipedia.org/wiki/Generic_Routing_Encapsulation

http://www.informit.com/articles/article.asp?p=605499&seqNum=10&rl=1

http://gathering.tweakers.net

http://nl.wikipedia.org/wiki/PPTP

http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx?mfr=true

http://www.schneier.com/pptp.html

http://support.bb4.com

http://nl.wikipedia.org/wiki/Prince2

http://technet2.microsoft.com/WindowsServer/nl/Library/b7ab88e6-9a6b-408a-a57b-698fe8b74aff1043.mspx?mfr=true

Papers:

KIVI & NGI, *ASI-Rapport*, 1995

Bijlage A: Definitieve opdrachtomschrijving

Danny Spaans

Kenmerk: DOA2006-2.1.70

Titel:
Ontwerpen van een virtuele omgeving bij Vanveen Informatica

Bedrijf:
Vanveen Informatica B.V. is een zelfstandige en onafhankelijke ICT-kennis-organisatie, actief vanaf 1987. Bij Vanveen informatica werken in totaal 37 mensen en bestaat uit drie businessunits:

Internet Security Consultancy.
Optional ICT-Support.
Network & User Services.

De kerncompetenties van de organisatie liggen op het ontwikkelen beheren en beveiligen van de infrastructurele kant van de ICT omgeving.

Probleemstelling:
Elke dag worden de bedrijfsnetwerken gemonitored. Er wordt doormiddel van het remote beheer protocol, via het internet, verbinding gemaakt met een server en vervolgens wordt alles gecontroleerd. Omdat dit een dagelijks procedure is, is dit een methode die veel tijd in beslag neemt.

De diversiteit aan hardware en software is groot. Dit maakt het monitoren van de hardware en software onoverzichtelijk.

Doelstelling:
Het ontwerpen van een virtuele omgeving tussen alle bedrijfsnetwerken, met daarbij passende monitoring software.

Uiteindelijk zal er een adviesrapport komen waarin een gedetailleerd ontwerp staat van een nieuwe netwerk infrastructuur.

In het kader van de afstudeeropdracht worden de volgende activiteiten verricht:

Definitiefase:
Oriëntatie bedrijf
Analyse huidige situatie
Opstellen plan van aanpak
Onderzoeken naar de mogelijke type netwerkverbindingen
Onderzoeken hoe een virtuele omgeving gerealiseerd kan worden
Onderzoeken van passende monitoring software
Opstellen oriënterend onderzoeksrapport

Architectuurfase:
Twee keuzes maken van de onderzochte netwerkverbindingen (een voorkeur en een alternatief)
Twee keuzes maken van de onderzochte monitoring tools (een voorkeur en een alternatief)
IP-adressering bepalen voor de virtuele omgeving
Tekening ontwerpen van de nieuwe netwerk infrastructuur.
Opstellen architectuur document.

Ontwerpfase:
Virtuele omgeving simuleren
Monitoring tools testen
Definitieve keuze maken van de netwerkverbindingen
Definitieve keuze maken van de onderzochte monitoring tools
Opstellen ontwerprapport.
Opstellen adviesrapport.
Inleveren afstudeerverslag
De volgende methodieken zullen gehanteerd worden:
Ontwerpmethode: ASI-rapport.

De volgende producten worden opgeleverd (De deelresultaten worden samengevoegd met informatie van een medestudent, dhr V. Schellevis):

Op te leveren producten
Plan van aanpak.(Definitiefase)
Oriënterend Onderzoekrapport.(Definitiefase)
Architectuurdocument.(Architectuurfase)
Ontwerpdocument.(Ontwerpfase)
Adviesrapport.(Ontwerpfase)

Bijlage B: Plan van aanpak

Inhoudsopgave

Voorwoord

Voor mijn afstudeerstage gaan mijn medestudent en ik een opdracht uitvoeren voor Vanveen informatica. De opdracht is in tweeën gedeeld om goed aan te kunnen tonen, wie wat gedaan heeft. Mijn deel is het ontwerpen van een virtuele omgeving en het onderzoeken van geschikte monitoring software. Ieder is verantwoordelijk voor eigen verslaglegging en uitvoering.

1 Inleiding

In dit document wordt als eerste de huidige situatie beschreven. Daarna volgt een overzicht van de probleemstelling, de doelstelling en werkwijze.
Vervolgens wordt een overzicht gegeven van de op te leveren producten, de mijlpalen en planning.

2 Achtergrond

Vanveen informatica is een zelfstandige en onafhankelijke ICT-kennis-organisatie, actief vanaf 1987. Bij Vanveen informatica werken in totaal 37 mensen en bestaat uit 3 business-units:
Internet Security Consultancy, Optional ICT-Support en Network & User Services.
De kerncompetenties van de organisatie liggen op het ontwikkelen, beheren en beveiligen van de infrastructurele kant van de ICT omgeving.

Internet Security Consultancy:
Bij Vanveen informatica zijn de consultants niet alleen in staat om een bedrijf te adviseren in de keuze van producten of inrichtingen daarvan, maar tevens ook in staat om deze operationeel te implementeren. Vervolgens hebben zij ook de specialisten in huis om de oplossingen te beheren.

Optional ICT-Support:
Vanveen informatica biedt ICT ondersteuning op maat aan, geheel passend bij de wensen en behoeften van het bedrijf. Desgewenst kan Vanveen informatica de zorg van een ICT-omgeving geheel op zich nemen. Vanveen informatica definieert samen met het bedrijf de mate waarin de ICT ondersteuning uitbesteed wordt in een ICT-zorgplan. De ondersteuning op maat ontstaat door het in kaart brengen van de verwachtingen van het bedrijf, het inventariseren van de bestaande ICT-omgeving en -processen, het uitwerken daarvan in het ICT-zorgplan, het implementeren van verbeteringen en het optimaliseren van het beheer.

Network & User Services:
Deze dienstverlening bestaat uit (project-)management, advies, ontwikkeling en implementatie. Met name heeft Vanveen informatica veel ervaring ten aanzien van het beheer, al dan niet conform ITIL, van complexe omgevingen. Ook kan de operationele gebruikersondersteuning worden verzorgd.

3 Huidige Situatie

Vanveen informatica heeft een aantal bedrijfsnetwerken van midden en klein bedrijven onder remote beheer. Deze service valt onder de afdeling Optional ICT-Support. Momenteel wordt er via het internet een aparte connectie gemaakt naar het netwerk van een bepaald bedrijf via het remote desktop protocol(RDP) of Virtual Computing Network(VNC). Op deze manier kunnen de servers worden benaderd en kan bijvoorbeeld het event log worden geraadpleegd. Verder wordt de back-up gecontroleerd d.m.v. het bekijken van de log files en worden monitoring tools gebruikt die op de servers geïnstalleerd staan om de hardware te zoals harde schijven, het werkgeheugen, netwerkkaarten etc. te monitoren.

Er bestaan verschillende contracten met de bedrijven in welke mate het beheer moet worden uitgevoerd en wat voor ondersteuning er geleverd wordt. Zo kan het zijn dat de kleinere bedrijven een onderhoudscontract hebben afgesloten voor wekelijkse controles, terwijl de grote bedrijven, met grotere omgevingen, dagelijkse controles willen hebben en onderhoud aan hun systemen.

Al deze bedrijven beschikken over hun eigen omgeving met veelal verschillende hardware en software. De connectie die nu wordt gemaakt naar de server wordt toegelaten door de firewall die de poort van het RDP protocol of VNC toelaat van een bepaald IP adres vanaf het internet.

4 Probleemstelling

Elke dag worden er bedrijfsnetwerken gemonitored doormiddel van het remote beheer protocol. Via het internet wordt er verbinding gemaakt met een server en vervolgens wordt alles gecontroleerd. Omdat dit een dagelijkse procedure is, is dit een methode die veel tijd in beslag neemt.

De diversiteit aan hardware en software is groot. De back-upsoftware verschilt per bedrijf en heeft zo zijn eigen methode om logs te kunnen uitlezen of versturen. De monitoring software die op de servers zijn geïnstalleerd om de hardware te controleren, wijkt ook af per server en per bedrijf. Dit maakt het monitoren van de hardware en software onoverzichtelijk.

5 Doelstelling

Er zal onderzocht worden wat de beste oplossing is om een virtuele omgeving te creëren, waardoor alle bedrijfsnetwerken virtueel aan elkaar worden gekoppeld. Hierdoor kunnen alle bedrijfsnetwerken centraal gemonitored worden.

Het vinden van passende monitoring software voor het centraal monitoren van alle servers in de bedrijfsnetwerken.

6 Opdrachtomschrijving

De opdrachtomschrijving is het onderzoeken van de best mogelijke oplossing van het ontwerpen van een virtuele omgeving tussen alle bedrijfsnetwerken, zodat alle netwerken vanaf één centraalpunt zichtbaar zijn.

Daarnaast is de taak ook om software te onderzoeken die het beste past in deze situatie en die alle bedrijfsnetwerken kan monitoren vanaf één punt. De software dient ook aan een aantal eisen te voldoen die later dit document beschreven worden.

Methode

Gedurende dit project hanteren wij de ontwikkel –en ontwerp methode ‘ASI-Rapport’. Deze methode is opgedeeld in de volgende fases:
- Definitiefase.
- Architectuurfase.
- Ontwerpfase.
- Ontwikkelfase.

Deze methode zorgt voor een gefaseerde aanpak voor het ontwikkelen van een technische infrastructuur. De ontwikkelfase laten we buiten beschouwing omdat wij ons niet bezighouden met implementeren van het ontwerp.

Het resultaat van de definitie fase is:
- een duidelijk beeld vormen van de huidige situatie.
- eisen en wensen aan de nieuwe situatie.
- oplossingsrichtingen om die nieuwe situatie te bereiken, inclusief de consequenties die hieraan vastzitten.
- Een voorkeursoplossing met een programma van eisen.
- Een globaal plan van aanpak voor het vervolg.

Om dit resultaat te bereiken moet allereerst veel informatie verzameld worden over de huidige situatie, plannen, wensen en harde eisen ten aanzien van de nieuwe situatie.

- Het resultaat van de architectuur fase is:
- Het bepalen van keuzes van de onderzochte resultaten
- Een netwerktekening van de netwerktopologie en netwerk componenten. Hierop staan ook de IP-ranges.
- Een alternatieve netwerktekening
- Architectuurdocument voor het vervolg van het project.

Het resultaat van de ontwerpfase is:

Testplan:
- Testen van de virtuele omgeving
- Testen van het monitoren binnen de virtuele omgeving

Het logisch ontwerp:
- gekozen standaarden en daarbinnen te hanteren opties/parameters voor de deelstructuren netwerken
- de samenhang en koppelingen tussen de deelstructuren en de componenten, binnen de deelstructuren; technieken en hulpmiddelen voor netwerkbeheer

Het ontwerp beheer/support:
- beschrijving configuratie
- gekozen producten

Werkwijze

Definitiefase:
Als eerste moet er een duidelijk beeld gecreëerd worden van de huidige situatie. Daarna wordt de eerste opzet van het plan van aanpak opgesteld. De eerste opzet zal verstuurd worden naar de opdrachtgever ter controle. Met de feedback van de opdrachtgever wordt het plan van aanpak gecorrigeerd en wordt uiteindelijk de final van het plan van aanpak ingeleverd.

Vervolgens wordt er onderzocht welke type netwerkverbindingen er zijn, die het mogelijk maken om de bedrijfsnetwerken virtueel met elkaar te verbinden. De bevindingen worden gedocumenteerd, daarna wordt er vergeleken met de huidige hardware en/of software van de bedrijven of deze type netwerkverbindingen worden ondersteund.

Wanneer er een lijst van alle mogelijke netwerkverbindingen is wordt er gekeken naar de huidige hardware en/of software van de bedrijven. Hier zal een lijst van op worden gesteld om dit later te kunnen vergelijken met het verdere onderzoek.

Daarna zal er gezocht worden naar passende monitoring software die bedrijfsnetwerken monitoren. De monitoring software moet van elke bedrijf het volgende kunnen constateren:

- Monitoren van Windows en Linux systemen
- Installatie op Windows en/of Linux
- Monitoren van de netwerkbeschikbaarheid
- Monitoren van hardware
- Monitoren van Windows event logs

- Monitoren van Linux syslogs
- Monitoren van Back-up software logs

De monitoring software die voldoet aan deze eisen zal worden gedocumenteerd. Dit kunnen ook meerdere zijn. Vervolgens wordt er gekeken of dit ook mogelijk is i.c.m. met de huidige hardware en/of software. Wanneer dit niet mogelijk is zal er gekeken worden welke hardware en/of software er aangeschaft moet worden om dit wel te realiseren is.

Alles wat onderzocht is zal worden opgesteld in het oriënterend onderzoekrapport

Architectuurfase:
In deze fase wordt er een keuze gemaakt welke type netwerkverbinding er gebruikt gaat worden, welke soort monitoring software en eventueel of er wel of geen hardware en/of software aangeschaft gaat worden.

Er wordt ook een netwerktekening gemaakt van de nieuwe situatie.

Ontwerpfase:
Als er een keuze is gemaakt zal de nieuwe situatie worden nagebootst doormiddel van een simulatieprogramma. De stappen die genomen zijn hoe de verbindingen in stand komen, zullen worden gedocumenteerd. Dit gaat beschreven worden in het ontwerpdocument.

Uiteindelijk zal er een adviesrapport worden opgeleverd. Het rapport beschrijft naar aanleiding van het onderzoek wat de best mogelijke oplossingen zijn om aan hun eisen en wensen te voldoen.

Er wordt ook een presentatie gemaakt en voorbereid en die zal in de laatste week gepresenteerd worden voor de medewerkers van Vanveen informatica. In deze presentatie wordt onder andere vertelt hoe het project is aangepakt, hoe de nieuwe situatie eruit zal gaan zien en hoe ze daar mee om moeten gaan.

7 Afbakening

De onderdelen die binnen het project vallen zijn:

- Het ontwerpen van een virtuele omgeving, tussen de verschillende bedrijfsnetwerken
- De virtuele omgeving moet toegankelijk zijn voor Vanveen
- Met een door mij geadviseerde monitoring tool moet het mogelijk zijn alle servers te monitoren conform de eisen van de opdrachtgever.

De onderdelen die buiten het project vallen:

- De beveiliging van de virtuele omgeving
- De implementatie van het ontwerp

Eisen

- Alle bedrijfsnetwerken moeten binnen één virtueel netwerk zichtbaar zijn
- Bedrijven kunnen onderling niet op elkaars netwerk komen.
- Monitoring software moet op de gebruikte platformen inzetbaar zijn
- De monitoring software moet gelijktijdig alle servers van de bedrijfsnetwerken kunnen controleren op de netwerkbeschikbaarheid, hardware(geheugen, harde schijven, processors etc.), Windows event logs en back-up logs
- De software bij klanten mag niet functioneel gewijzigd worden
- Er mogen geen hardware aanpassingen komen bij klanten.

8 Op te leveren producten

- Plan van aanpak
- Onderzoekrapport
- Architectuurdocument
- Ontwerpdocument
- Adviesrapport

9 Planning

Week	Fase	Startdatum/einddatum	Activiteiten
1	Definitiefase	4-9-2006/8-9-2006	- Kennismaken - Huidige situatie bekijken - Opstellen deel van pva
2	Definitiefase	11-9-2006/15-9-2006	- Eerste concept pva inleveren - Onderzoeken naar de mogelijkheden om een virtuele omgeving te creëren
3	Definitiefase	18-9-2006/22-9-2006	- Onderzoeken naar de mogelijke type VPN-verbindingen - Pva final inleveren
4	Definitiefase	25-9-2006/29-9-2006	- Onderzoeken naar de mogelijke type VPN-verbindingen - De gevonden mogelijkheden documenteren - pva verbeteren en verder uitbreiden
5	Definitiefase	2-10-2006/6-10-2006	- Onderzoek naar beschikbare monitoring tools. - bevindingen documenteren
6	Definitiefase	9-10-2006/13-10-2006	- Onderzoek naar beschikbare monitoring tools. - Bevindingen documenteren - Oriënterend onderzoeksrapport inleveren
7	Architectuurfase	16-10-2006/20-10-2006	- Gesprek met examinatoren - Keuzes maken van de onderzochte resultaten
8	Architectuurfase	23-10-2006/27-10-2006	- Keuzes maken van de onderzochte resultaten - Definitieve opdrachtomschrijving inleveren
9	Architectuurfase	30-10-2006/3-11-2006	- Voorkeursoplossingen verder uitwerken - Onderzoeken welke eventuele hardware aangeschaft moet worden - Voortgang verslag inleveren voor school
10	Architectuurfase	6-11-2006/10-11-2006	- IP-adressering bepalen van de nieuwe situatie - Blauwdruk(tekening) ontwerpen van de nieuwe netwerk infrastructuur
11	Architectuurfase	13-11-2006/17-11-2006	- Blauwdruk(tekening) ontwerpen van de nieuwe netwerk infrastructuur
12	Ontwerpfase	20-11-2006/24-11-2006	- Inleveren concept architectuurdocument
13	Ontwerpfase	27-11-2006/1-12-2006	- Virtuele omgeving simuleren en testen
14	Ontwerpfase	4-12-2006/8-12-2006	- Virtuele omgeving simuleren en testen - gedetailleerde bouwplan inleveren voor school
15	Ontwerpfase	11-12-2006/15-12-2006	- Testen van de monitoring tool via de virtuele omgeving
16	Ontwerpfase	18-12-2006/22-12-2006	- Testen van de monitoring tool via de virtuele omgeving - inleveren ontwerpdocument
17	Ontwerpfase	2-1-2006/5-1-2006	- Afronden afstudeerverslag - Presentatie maken
18	Ontwerpfase	8-1-2006/12-1-2006	- inleveren adviesrapport - Presentatie presenteren aan het personeel afstudeerverslag inleveren

10 Mijlpalen

Week	Fase	Op te leveren documenten
3	Definitiefase	Plan van aanpak
8	Definitiefase	Onderzoeksrapport, definitieve opdrachtomschrijving
12	Architectuurfase	Architectuurdocument
15	Ontwerpfase	Ontwerpdocument
18	Ontwerpfase	Adviesrapport, presentatie, afstudeerverslag