Afstudeerscriptie

Remote Management

Versie:	3.0
Datum:	15-12-2009

Auteur:	Mark Laurens Bolten
Studentnummer:	1520411
Telefoonnummer:	06 19098592
E-mail:	mark.bolten@student.hu.nl
Opleiding:	Systeembeheer voltijd
Eerste examinator:	Kees Uiterwijk

Bedrijfsnaam:	igilde
Adres:	Tolnasingel 1 2411 PV Bodegraven
Internetadres:	www.igilde.nl
Telefoon	0172 766000

Voorwoord

Dit document is opgesteld als afstudeeropdracht voor de opleiding systeembeheer aan de Hogeschool Utrecht in de periode van september 2009 tot januari 2010.

In deze periode moet de afstudeerder het bewijs leveren dat er genoeg kennis is opgedaan tijdens de opleiding en dit ook in de praktijk kan toepassen. Om die reden is er contact gelegd met igilde en is de afstudeeropdracht tot stand gekomen. Dit heeft geleid tot een overeenstemming en na goedkeuring van de Hogeschool Utrecht is de opdracht uitgevoerd conform een werkweek van 40 uur in de genoemde periode.

Mijn dank gaat uit naar: Winitu en igilde die het afstuderen mogelijk hebben gemaakt met in het speciaal:

Irene Postema: waarmee het contact is ontstaan

Kees van Rooden: waarmee de afstudeeropdracht tot stand is gekomen en tevens begeleider

Ruud van den Oosterkamp: waarmee tevens de afstudeeropdracht tot stand is gekomen

Ook gaat mijn dank uit naar de begeleider van de Hogeschool Utrecht: **Kees Uiterwijk**.

In deze afstudeerscriptie is te lezen wat er precies gedaan is tijdens het uitvoeren van de opdracht bij igilde. De voorbereiding, de aanpak, de uitvoering en het uiteindelijke resultaat.

Management samenvatting

igilde wil op gebied van remote beheer een stap vooruit gaan. Met remote beheer wordt in dit document bedoeld: het op afstand hulp bieden en onderhoud plegen aan de computers en netwerken van klanten. igilde ondervindt op dit gebied problemen wat veel tijd vergt en is daarom dit project gestart.

In deze scriptie over remote beheer is beschreven wat er onderzocht is en wat de bevindingen waren. Hieruit zijn een aantal conclusies getrokken waarna de adviezen voor igilde zijn opgesteld.

De opdracht zoals deze is opgesteld samen met igilde luidt als volgt: “Ontwerp een gestandaardiseerd proces voor het uitvoeren van remote beheer” waarbij er gefocust is op de veiligheid van de oplossing. Hierbij moet onder andere gedacht worden aan: hoe om te gaan met accounting en het versleutelen van het dataverkeer.

igilde heeft eisen en wensen opgesteld waaraan een nieuwe oplossing moet voldoen. Dit zijn de punten waar igilde tegenaan loopt en verbetering wil hebben om haar klanten betere service te kunnen bieden.

De eisen en wensen zijn fundamentele informatie die gebruikt zijn voor het opzetten van het onderzoek naar mogelijke oplossingen.

In een later stadium is er overeengekomen dat er drie mogelijke implementaties opgesteld zijn hoe igilde het remote beheer kan implementeren. De implementaties zijn voortgekomen uit de software pakketten die onderzocht zijn. Hier is een top drie uitgekomen waarvoor de implementaties geschreven zijn. In deze implementaties is beschreven welke stappen ondernomen moeten worden om remote beheer tussen de netwerken van igilde en de klanten zo optimaal mogelijk uit te kunnen voeren. Tevens wordt er beschreven wat er binnen het netwerk van igilde gedaan kan worden om de veiligheid te verhogen.

Inhoudsopgave

1 Beschrijving van de organisatie

1.1 igilde

igilde is een full service IT dienstverlener met een sterke focus op netwerktechnologie ten behoeve van Service Providers, Telecom partijen, grootzakelijke klanten en het MKB.

igilde is een nieuwkomer in de sector en staat voor vakmanschap, kwaliteit, vertrouwen en slagvaardig handelen. Met een vracht aan internationale ervaring in zowel de telecom/ISP-wereld als in het bedrijfsleven bouwt en optimaliseert igilde systemen met als ultieme doel het behalen van competitief voordeel van hun klanten.

igilde levert niet alleen hardware inclusief diverse financieringsmogelijkheden maar igilde verzorgt het complete spectrum van ontwerp tot complete implementaties inclusief alle benodigde IT systemen en processen. Ook vergelijkende testen, second opinions, monitoren en beheer vormen een onderdeel van het portfolio van igilde.

Zoals eerder genoemd werkt igilde met een sterk team en bieden zij voldoende mogelijkheden tot begeleiding van afstudeerders wat veel vertouwen schept. De Winitu groep waar igilde deel uit maakt, heeft rond de 30 werknemers die goed met elkaar samenwerken in gezamenlijke kantoorruimtes. Dit bevordert de communicatie en werkt prettig.

De adresgegevens van het bedrijfspand zijn:

Tolnasingel 1
2411 PV Bodegraven

1.2 Positie van de afstudeerder

In september 2009 is de afstudeerder bij igilde begonnen als onderzoeker/adviseur op het NOC (Network Operations Center). Dit is een kleine afdeling waar alles omtrent het beheer van klantnetwerken tot klantsystemen wordt afgehandeld. Hij werkte hier in een kantoorruimte waar zich nog 2 á 3 medewerkers van deze afdeling bevinden. Dit varieert omdat medewerkers ook op locatie bij de klant kunnen zijn. Er zijn twee specialisten en één iemand van de HR aangewezen als begeleiding. Binnen de afdeling is een eigen werkplek toegewezen met een internet en telefoonverbinding en het is voorgekomen dat de telefoon aangenomen moest worden en de klant te woord gestaan is. Zo is er kennis gemaakt met de manier van werken en verwerken binnen igilde.

De afstudeerder was vrij om te kiezen met welk besturingssysteem hij wilde werken omdat er genoeg kennis in huis is en de systemen naadloos op elkaar aansluiten en samenwerken. Bij het uitvoeren van de werkzaamheden was het gebruik van een eigen laptop akkoord.

De collega's op de afdeling houden zich bezig met het testen van nieuwe systemen, het beheren van netwerken en het aannemen, registreren en soms direct oplossen van incidenten via binnenkomende telefoon gesprekken en e-mail berichten.

2 Het project

2.1 Inleiding en achtergrond

igilde is een kleine snel groeiende onderneming. Om klanten nog beter te bedienen zijn er een aantal punten die igilde toe wil voegen aan de dienstverlening maar waar ze zelf niet aan toe komen omdat het geen hoge prioriteit heeft. Één daarvan is dat ze een gestandaardiseerde veilige mogelijkheid willen hebben om remote beheer uit te voeren. igilde maakt momenteel al gebruik van remote beheer alleen gaat hier te veel fout wat wantrouwen en irritaties opwekt bij de klanten.

De klanten van igilde variëren van 10 tot 150 werkplekken. Hierbij horen uiteraard ook de randapparatuur, de netwerkcomponenten en de servers om deze hoeveelheid werkplekken operationeel te houden. Naast MKB klanten werkt igilde ook voor internet providers waar verschillende eenheden in grote aantallen voorkomen, zoals: 300 tot 400 routers/switches/dns-servers en dhcp servers. Deze aantallen zullen volgens de verwachtingen met de jaren mee alleen maar stijgen.

Omtrent remote beheer zijn er geen duidelijke richtlijnen en checklists opgesteld waardoor er regelmatig geen remote beheer kan plaatsvinden. Het wordt snel ingesteld met de intentie dat het werkt. Echter blijkt het dat er vaak instellingen vergeten zijn waardoor het niet werkt, mede omdat het niet getest wordt. Ook wordt er bij deze acties niet nagedacht of het veilig is om remote beheer in te stellen.

Het gebeurt daarom te vaak dat het toch noodzakelijk is om naar de klant toe te gaan. Naar de klant toegaan, betekent dat lopende zaken tijdelijk stil gelegd worden om de werkzaamheden bij de klant uit te kunnen voeren die op dat moment een hogere prioriteit hebben. igilde heeft klanten door heel het land waardoor er soms lange reistijden zijn om naar de klant toe te gaan, voornamelijk tijdens de spitsuren. Uiteindelijk blijkt het probleem vaak gemakkelijk op te lossen en is er onnodige tijd verloren gegaan. Om dit te voorkomen zou het een ideale oplossing zijn om dit soort werkzaamheden uit te kunnen voeren vanaf de locatie waar de werknemer zich op dat moment bevindt om daarna direct zijn andere werkzaamheden op te kunnen pakken. Om dit te realiseren wil igilde een advies over hoe dit het beste gerealiseerd kan worden en wat de mogelijkheden en onmogelijkheden zijn waarbij veiligheid een belangrijk aandachtspunt dient te zijn.

De te beheren componenten zijn onder andere:

1. Servers
2. Werkstations
3. Netwerkcomponenten
    a. Routers
    b. Switches
    c. VOIP telefoons
    d. VOIP centrales
    e. Draadloze Accespoints

2.2 Formulering

Gedurende het project is er een ontwerp gemaakt voor het remote beheer voor igilde. Hoe doet igilde dit momenteel en hoe kan dit in de toekomst verbeterd worden. Hierna is er onderzocht wat de mogelijkheden en onmogelijkheden zijn van het remote beheer waarbij goed nagedacht is over:

- Hoe om te gaan met accounts ten behoeve van beheer?
- Hoe om te gaan met beheer van werkstations?
- Wat voor hard-/software is nodig voor het remote beheer?
- Wat zijn de mogelijkheden van de mobiele technieken als GPRS/HSDPA?

Uiteindelijk is daar een rapport uitgekomen waaruit een beeld geschept kan worden wat de do's en don't zijn omtrent remote beheer en waar rekening mee gehouden moet worden als de klant remote beheerd dient te worden. Hierbij is gedacht aan:

- IP adressering
- Installeren/configureren van benodigde software/hardware
    - Routers
    - Modems
- Configureren van veilige verbindingen
- Aanmaken van benodigde gebruikers

Hieruit zijn een drietal adviezen voortgekomen waaruit er één gekozen kan worden die nagelopen dient te worden als het netwerk van een klant geconfigureerd wordt voor remote beheer.

Bij het eindresultaat is rekening gehouden met schaalbaarheid zodat het zowel voor kleinere als voor grote klanten inzetbaar is.

2.2.1 Doelstellingen

De doelstellingen binnen dit project waren als volgt:

- Inventariseer de huidige methode van remote management
- Onderzoek de huidige technieken omtrent remote beheer
- Ontwerp een gestandaardiseerd proces voor het uitvoeren van remote beheer

2.2.2 Gebruikte methoden en technieken

De technieken die tijdens het project gebruikt zijn, zijn als volgt:

De projectmethode Prince2 is gebruikt voor dit project. Prince2 is een zeer uitgebreide projectmethodiek voor het uitvoeren van grote projecten waar onder anderen veel projectleden aan te pas komen. Bij dit project zijn om die reden slechts aantal aspecten van Prince2 gebruikt:

- Project Brief
- Project Initiation Document
- Faseren van het project en activiteiten opdelen in deelactiviteiten
- Alleen de elementen Projectgroep(afstudeerder) en project board (opdrachtgever) worden benoemd
- Wekelijkse update over de status van het project

Tijdens het project zijn een aantal technieken naar voren gekomen waar kennis mee gemaakt is en veel over geleerd is:

- Remote beheer met de verschillende protocollen en mogelijkheden
- VPN
- Beveiligde verbindingen
- Firewall
- Gebruikersbeheer
- Verbindingsmogelijkheden om tijdens calamiteiten nog steeds remote beheer uit te kunnen voeren.
    - ISDN
    - GPRS/HSDPA
    - ADSL

2.2.3 Projectactiviteiten

De activiteiten die het project omvatten om het eindresultaat te kunnen behalen zijn:

1. Opstellen van Plan van Aanpak voor de uitvoering van het project
2. Onderzoeken van huidige manier van remote beheer
3. Onderzoeken van huidige mogelijkheden van remote beheer
4. Testen van een selectie mogelijkheden met de benodigde resources
5. Verwerken van de testresultaten
6. Gestandaardiseerde oplossing voor remote beheer ontwerpen
    a. Inrichting van de infrastructuur (Hardware/Software)
    b. Checklist die nagelopen moet worden om een klant klaar te maken voor remote beheer
7. Adviesrapport opstellen waarin de do's en dont's van het remote beheer naar voren komen en waar een keuze wordt gemaakt voor de beste oplossing
8. Alles verwerken in de afstudeerscriptie
9. Presentatie aan werknemers van Winitu/igilde
10. Afstudeerzitting om de uitvoering en resultaten van de opdracht te presenteren

2.2.4 Afspraken

Voor dit project zijn tussen de opdrachtgever (igilde) en afstudeerder (Mark Bolten) een aantal afspraken gemaakt:

- Het afstudeercontract loopt van 01-09-2009 tot eind januari 2010
- De afstudeerder werkt 8 uur per dag tussen 7:30 en 18:30
- Afstudeerder voert soms lichte werkzaamheden uit binnen het bedrijf, bijvoorbeeld het aannemen van de telefoon
- De afstudeerder krijgt een eigen werkplek met computer
- Communicatie vindt plaats telefonisch, via mail of op kantoor
- Als de afstudeerder genoodzaakt is om op school aanwezig te zijn kan dit tijdens de werktijd plaatsvinden

2.2.5 Scope

De scope van het project geeft aan welke werkzaamheden binnen het project vallen en welke niet. Door het goed opstellen van de scope worden onduidelijkheden gedurende het project voorkomen.

2.2.5.1 Binnen de scope

- Onderzoeken van de huidige situatie
- Onderzoeken van de huidige technieken van remote beheer voor de volgende componenten
    - Servers (Windows/Linux)
    - Desktops (Windows/Linux)
    - Switches
    - Routers
    - Printers
- Tijdens het onderzoek dient er aandacht besteed te worden aan de in dit document vermelde technieken
- Testen van de onderzoeksresultaten in een testomgeving
- Ontwerpen van standaardiseerde oplossing voor remote beheer van de genoemde componenten
- Presenteren van de resultaten aan de werknemers van igilde

2.2.5.2 Buiten de scope

- Het implementeren van een oplossing

3 Aanpak en fasering

Het project is opgedeeld in zes fases. Hierdoor is het overzicht goed bewaard en was er goed inzicht in de voortgang. In tabel 1 is te zien wat de doorlooptijd van de fases was en in de paragraaf die daarop volgt is elke fase kort toegelicht.

Fase nummer	Naam	Startdatum	Einddatum
1	Opstartfase	01-06-2009	28-08-2009
2	Initiatiefase	31-08-2009	11-09-2009
3	Onderzoeksfase	21-09-2009	20-11-2009
4	Testfase	23-11-2009	11-12-2009
5	Ontwerpfase	14-12-2009	12-01-2010
6	Afsluitfase	13-01-2010	15-01-2010

Tabel 1: Doorlooptijd van de fases

3.1 Fase 1: Opstartfase

In de opstartfase is er middels een afstudeervoorstel toestemming gevraagd aan de examencommissie van de Hogeschool Utrecht om dit project uit te voeren. Hiervoor zijn een aantal informatiemomenten georganiseerd om goed op de hoogte te zijn wat de Hogeschool Utrecht hiervan verwacht. Na goedkeuring van het afstudeervoorstel is de afstudeerder met zijn project begonnen.

De activiteiten in deze fase waren:

- Vinden van een afstudeeropdracht
- Opstellen van het afstudeervoorstel
- Goedkeuring van het afstudeervoorstel

3.2 Fase 2: Initiatiefase

In de initiatiefase zijn alle voorbereidingen getroffen om aan het project te beginnen. Zoals het opstellen van de projectplanning.

De activiteiten in deze fase waren:

- Ontwerpen van een document sjabloon
- Opstellen van het Project Initiation Document
- Opstellen van de Projectplanning

3.3 Fase 3: Onderzoeksfase

In deze fase heeft het onderzoek plaatsgevonden met de daarbij behorende rapportages waarin de resultaten te zien zijn.

De activiteiten in deze fase waren:

1. Onderzoeken van de huidige situatie
    a. Interviews met betrokkenen
    b. Netwerkinfrastructuur in kaart brengen
    c. Huidige situatie beschrijven
2. Onderzoeken van de huidige technieken omtrent remote beheer
    a. Onderzoek huidige aanbod van remote beheer applicaties
    b. Selectie maken aan de hand van de onderzoeksresultaten
    c. Onderzoek de huidige beveiligingstechnieken omtrent remote beheer
    d. Beschrijven van de onderzochte beveiligingsaspecten

3.4 Fase 4: Testfase

In deze fase zijn de onderzoeksresultaten uitgebreid getest en beoordeeld.

De activiteiten in deze fase waren:

3. Testen van de geselecteerde applicaties
    a. Beoordelen van de testresultaten
    b. Top drie maken aan de hand van de beoordelingen
    c. Beschrijven van de mogelijke oplossingen

3.5 Fase 5: Ontwerpfase

In de ontwerpfase is het daadwerkelijke ontwerp gemaakt waarin een aantal mogelijke procedures ontwikkeld zijn voor het opzetten van remote beheer van klanten.

De activiteiten in deze fase waren:

1. Ontwerpen van drie scenario's (procedures) voor het opzetten van remote beheer
2. Beschrijven van de adviezen

3.6 Fase 6: Afsluitfase

In de afsluitfase gaat de afstudeerder het werk presenteren aan de werknemers van igilde en wordt de scriptie overhandigd aan de opdrachtgever. Hogeschool Utrecht ontvangt tevens de scriptie ter beoordeling waar de afstudeerzitting op zal volgen. Als alles correct is afgesloten behaalt de afstudeerder zijn diploma en heeft igilde een mooi eindresultaat waarmee zij verder kunnen.

De activiteiten in deze fase zijn:

- Afronden afstudeerscriptie
- Presentatie aan de werknemers van igilde
- Afstudeerzitting op de Hogeschool Utrecht

3.7 Projectplanning

De gedetailleerde projectplanning is bijgevoegd in bijlage 1.

4 Uitgangssituatie

Om een goed inzicht te krijgen is er onderzocht hoe igilde op dit moment remote beheer uitvoert. Dit is gebeurd doormiddel van een aantal gesprekken met de opdrachtgever die uitleg heeft gegeven over de huidige manier van werken en hoe de infrastructuur er uitziet met de bijbehorende tekeningen.

Daarna zijn er een aantal interviews gehouden met zowel de opdrachtgever als medewerkers van igilde. In deze interviews zijn nogmaals vragen gesteld over de huidige manier van werken maar meer gericht op het remote beheer. Daarnaast zijn er vragen gesteld over de tevredenheid van de huidige manier van werken en wat ze hier graag aan willen verbeteren.

Ook zijn er al een aantal globale oplossingen voorgehouden om te bepalen in welke richting gezocht moest worden.

4.1 Interviewvragen

Tijdens de interviews zijn de volgende vragen gesteld:

1. Wordt er op dit moment binnen igilde al gebruik gemaakt van remote beheer?
2. Welke technieken worden hierbij gebruikt?
3. Worden er momenteel alleen servers en desktops remote beheerd?
4. Vindt u het beheren via web interfaces, telnet of SSH handig?
5. Bent u tevreden met de huidige manier van remote beheren?
6. Ondervindt u veel problemen met het remote beheer? Missen van functionaliteiten, uitval van de dienst, snelheid, wachtwoord vergeten etc.?
7. Wat zou u graag anders zien wat betreft de huidige manier van remote beheren?
8. Zou u het handig vinden om een totaalpakket te hebben om remote beheer te kunnen doen? En is igilde bereid om hier (veel) geld aan uit te geven of ligt de voorkeur bij freeware?
9. Moet die oplossing platformonafhankelijk zijn?
10. Er zal waarschijnlijk geen totaalpakket bestaan voor het beheren van Windows en Linux machines. Wat vindt u er van om voor de Windows machines een dergelijke oplossing te gebruiken en om de Linux machines via de huidige manier te beheren?
11. Moet het mogelijk zijn om remote beheer vanaf de mobiele telefoon uit te voeren? Of via de laptop via de wat trage internet verbinding van de mobiele telefoon?
12. Wat vindt u van een oplossing als logmein.com of teamview?
13. Wat vindt u van een oplossing om bij elke klant één pc in te richten met verschillende beheer tools en dat daar een VPN verbinding mee opgebouwd wordt om vanaf daar het volledige netwerk te kunnen beheren?

4.1.1 Samenvatting van de antwoorden

De antwoorden op de vragen waren vrij eenzijdig. Er is geen overzicht weergegeven van de individuele antwoorden maar een samenvatting hiervan. In de volgende paragraaf is dit in de vorm van een verhaal uitgewerkt.

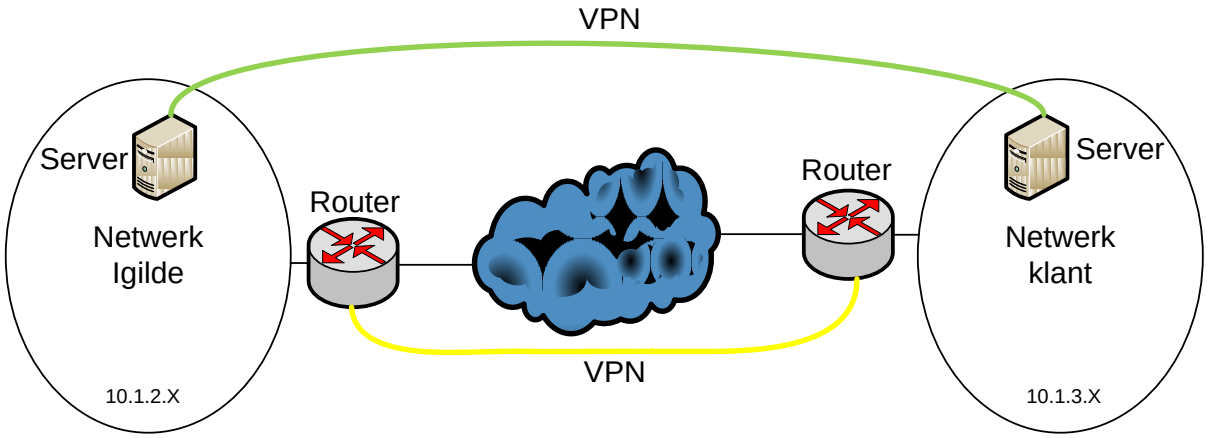
1. Ja, de werknemers van het NOC maken gebruik van remote beheer om klanten te ondersteunen.
2. De technieken die wij gebruiken zijn: voor Windows machines: RDP, voor Linux machines: SSH en voor de routers/switches: telnet. VMware console wordt gebruikt om verbinding te maken met de virtuele infrastructuren en voor overige apparaten worden vaak webinterfaces gebruikt. Naar de klanten liggen IPsec beveiligde VPN verbindingen waar deze datastromen overheen gaan.
3. Naast servers en desktops beheren wij ook laptops, routers, switches, printers en modems.
4. Ja, Linux systemen zijn gemakkelijk te beheren via SSH net zoals dat het handig is dat routers en switches via een telnet sessie benaderbaar zijn.
5. Nee, wij zijn niet tevreden met de huidige situatie, er kan gesteld worden dat het “quick en dirty” is opgezet. De VPN verbindingen zorgen er onder andere voor dat er verkeer mogelijk is tussen igilde en haar klanten wat ook betekent dat de klanten vanaf hun locatie op het netwerk van igilde kunnen komen, dat is iets wat niet zou mogen. Daarbij is de beveiliging zo ingesteld dat iedereen het netwerk van de klant op kan. Echter alleen op IP basis en niet op DNS naam omdat deze niet bekend zijn op het lokale netwerk van igilde.
6. Ja, het gaat wel regelmatig fout. Het gebeurt zelden dat er een VPN verbinding tijdelijk wegvalt door een internet storing. Soms is er te weinig bandbreedte waardoor het remote beheer heel traag is. Het kom ook regelmatig voor dat we het wachtwoord van de gebruiker niet weten en dat we niet in kunnen loggen. Het moet niet nodig zijn het wachtwoord van de klant te weten.
7. De volgende mogelijkheden zouden we graag willen hebben:
    a. De gebruiker kan meekijken, het scherm wordt niet vergrendeld.
    b. De gebruiker krijgt een melding waarbij hij toestemming moet geven om remote beheer toe te staan.
    c. Alleen gemachtigde mogen verbinding maken met het netwerk van de klant.
    d. Gebruikers van het klantnetwerk mogen geen verbinding maken met het netwerk van igilde maar het moet wel mogelijk zijn om de systemen te monitoren, dit verkeer moet daarom toegestaan worden.
8. Een totaalpakket zou wel heel handig zijn maar denk dat, dat niet bestaat. Een vergelijking van betaalde pakketten tegenover freeware is gewenst.
9. Het is niet heel hard nodig om een platform onafhankelijke oplossing te hebben omdat de klanten voornamelijk Windows systemen gebruiken en dit voldoende zal zijn.
10. Het zal handig zijn als er een pakket te vinden is waarin alles kan maar het is geen probleem om voor verschillende systemen verschillende beheersmogelijkheden te hebben. Webmin is geen handig alternatief, alleen voor gebruikers met weinig Linux ervaring.

11. Nee, het is niet nodig dat vanaf het scherm van de mobiele telefoon verbinding gemaakt kan worden naar de netwerken van de klanten. Wel graag rekening houden met de bandbreedte die nodig is waardoor bij nood vanaf de laptop via de telefoon toch een redelijke verbinding opgezet kan worden.
12. Nee, oplossingen als logmein.com of teamview ziet igilde niet als gewenste situatie.
13. Het inrichten van een beheer pc lijkt een goede oplossing. Hierdoor neem je al heel wat problemen weg omdat er met accounting gemakkelijk ingesteld kan worden wie er op dat systeem mag inloggen. Zodra dat al niet mag is de rest van het netwerk afgeschermd. Of dit station zich bij de klant bevindt of bij igilde zelf maakt niet uit. Het zou mooi zijn als het mogelijk is om bij igilde één systeem te hebben die de toegang tot de klantnetwerken verleend of één systeem die meerdere klanten bedient.

4.2 Omschrijving van de huidige situatie

Aan de hand van de interviews en de verstrekte informatie is de huidige situatie geschetst.

Om ondersteuning aan de klanten van igilde te bieden wordt er al gebruik gemaakt van remote beheer. igilde verstaat onder remote beheer het overnemen van de systemen van de klant om ondersteuning te bieden of een probleem op te lossen. De IPsec beveiligde VPN verbindingen met de klanten zorgen ervoor dat het netwerk van igilde gekoppeld wordt aan het netwerk van de klant. Afhankelijk van de klant wordt er een VPN sessie opgezet tussen Cisco routers of Windows servers.



Figuur 1: Huidige opbouw van de VPN verbindingen

De klanten hebben voor igilde unieke private IP adressen gekregen zoals in figuur 1 te zien is om IP adres conflicten te voorkomen.

Via de VPN verbinding is er intern dataverkeer mogelijk tussen de twee netwerken en kunnen de systemen van de klant benaderd en gemonitord worden. Iedereen die zich op het igilde netwerk bevindt kan dit doen. Er kan echter alleen op de systemen ingelogd worden als de inloggegevens bekend zijn. Het is overigens ook mogelijk om vanaf het netwerk van de klant op het igilde netwerk te komen. Dit is niet veilig omdat het dan mogelijk is dat gegevens van igilde in handen komen van hun klanten.

De Windows systemen worden overgenomen doormiddel van het RDP (remote desktop protocol) protocol. Dit zit geïntegreerd in de besturingssystemen van Microsoft en maakt het mogelijk om de huidige sessie van een computer over te nemen. Een nadeel van RDP is dat het over te nemen systeem vergrendeld wordt zodra de verbinding tot stand is gebracht en de klant niet mee kan kijken met wat de beheerder doet. Daarbij moet het wachtwoord van de gebruiker bekend zijn of uitgewisseld worden om in te loggen op de actieve sessie. Als er ingelogd wordt als beheerder wordt deze namelijk afgemeld wat erg onhandig is. Voor servers is dit wel een prima oplossing want dan is het juist de bedoeling dat de server vergrendeld wordt en er niemand mee kan kijken.

De Linux machines, wat alleen servers zijn worden beheerd via SSH waar de werknemers van igilde tevreden over zijn. De routers en de switches worden via telnet of SSH beheerd, dit is voor igilde de enige werkbare methode.

De huidige situatie heeft zowel voor- als nadelen die hieronder zijn opgesomd:

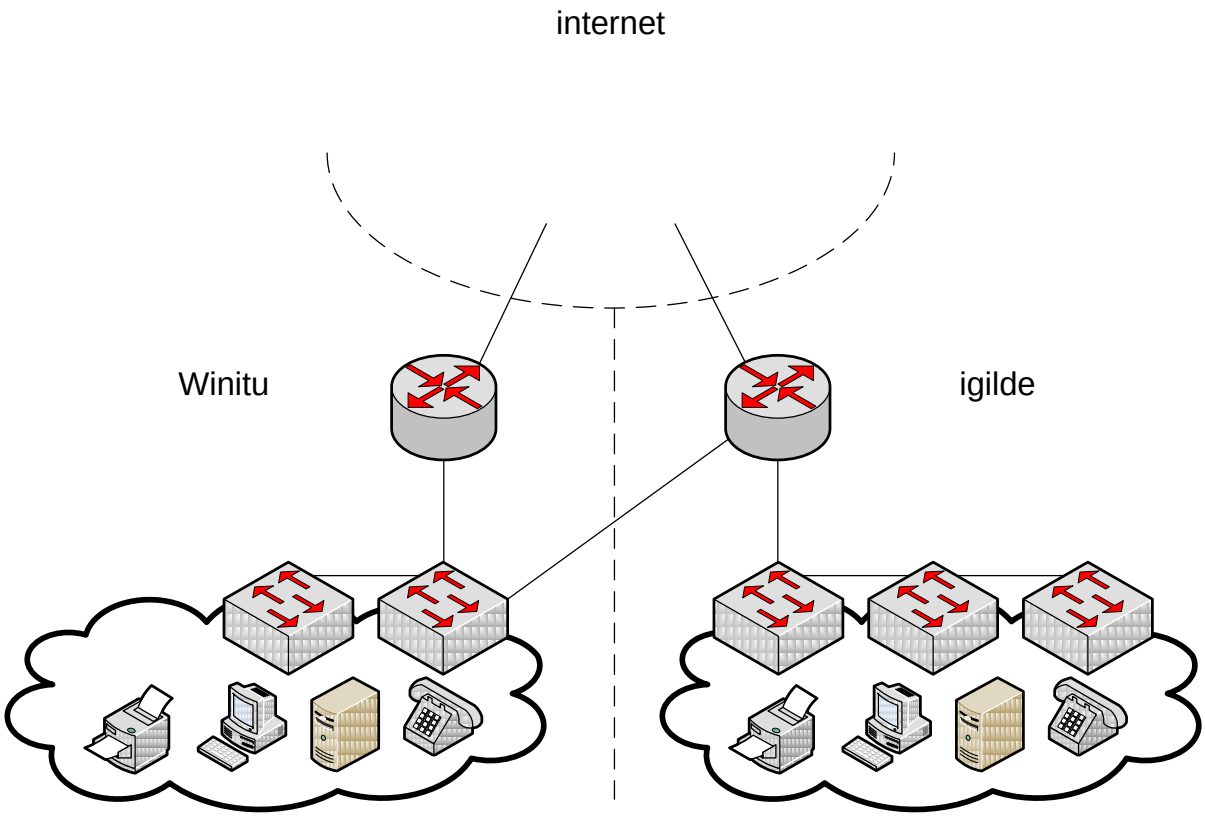
- Voordelen:
  - Geen beveiligingsbelemmeringen
    - Binnen het netwerk van igilde kan er altijd beheer uitgevoerd worden
  - Geen interactie met de klant nodig voor het overnemen van het scherm
- Nadelen:
  - Klant kan niet meekijken en ziet alleen een inlogscherm
  - Klanten kunnen alle resources binnen het netwerk van igilde bereiken
  - Klanten kunnen ook resources op het netwerk bereiken die niet van toepassing zijn
  - Klant ziet zijn scherm verspringen en weet niet of de beheerder nog bezig is, of hij al klaar is of wat er überhaupt gebeurt
  - De klant moet zijn wachtwoord doorgeven aan de beheerder zodat hij in kan loggen

igilde wilde in het eindresultaat dat de volgende punten mogelijk zijn:

- Alleen beheerders hebben toegang tot de netwerken van de klanten
- Klanten kunnen het netwerk van igilde niet bereiken
- Klanten kunnen meekijken met het beheer, ze zien de muis bewegen en weten wat er gebeurt
- Er kan ingelogd worden doormiddel van een beheerderwachtwoord waardoor het niet nodig is het wachtwoord van de klant te weten

4.3 Globaal overzicht van het netwerk

Het netwerk is opgedeeld in twee segmenten waarbij er één segment gebruikt wordt voor Winitu en het andere segment voor igilde. Winitu is het moederbedrijf van igilde. De twee segmenten zijn aan elkaar gekoppeld doormiddel van statische routes tussen de routers. De reden hiervoor is dat de apparatuur zich op dezelfde locatie bevindt en er verkeer tussen de twee netwerk mogelijk is zonder NAT te gebruiken.



Figuur 2: Netwerkoverzicht Winitu groep

Een uitgebreidere tekening verstrekt door igilde is terug te vinden in bijlage 2.

4.4 Gewenste situatie

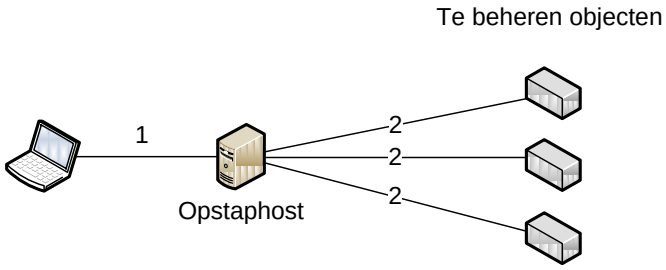
Nadat de huidige situatie geanalyseerd is, is er een omschrijving gemaakt waaraan de gewenste situatie moet voldoen.

De gewenste situatie moet dusdanig worden opgezet dat de VPN verbindingen naar de klanten afgeschermd worden. De protocollen voor het overnemen van een extern scherm, syslog berichten en SNMP moeten minimaal toegang hebben tussen het netwerk van igilde en de klanten. igilde maakt gebruik van Nagios® en Cacti om hun eigen systemen en de systemen van de klanten te monitoren. Hiervoor moeten syslog en SNMP berichten toegestaan worden.

Daarnaast is het gewenst om het igilde netwerk zo in te richten dat alleen beheerders toegang hebben tot de netwerken van de klanten.

Een opstaphost die goed beveiligd is kan handig zijn omdat hiermee al heel veel beveiligingsrisico's worden voorkomen, de VPN verbindingen misschien niet meer nodig zijn en alle benodigde beheer tools vanaf deze computer beschikbaar zijn om eenvoudig ondersteuning te bieden.

Met opstaphost wordt een computer of bedoeld waar eerst op ingelogd moet worden. Vanaf deze machine wordt vervolgens toegang verleend aan het netwerk van de klant.



Figuur 3: Opstaphost

Het moet niet nodig zijn om het wachtwoord van de gebruiker te weten wanneer er ondersteuning geboden moet worden, dit zou mogelijk moeten zijn met het administrator wachtwoord van het netwerk. Dan moet het wel zo zijn dat de gebruiker een melding krijgt waarop gevraagd wordt of remote beheer gewenst is en dit dan kan toestaan of afwijzen. Voor de cliënts moet het mogelijk zijn dat de klant mee kan kijken op het scherm wat er gebeurt, niet dat de gebruiker naar een vergrendeld scherm zit te kijken en zit te wachten tot de beheerder het probleem heeft opgelost. De mogelijkheid om de externe invoerapparaten (muis/toetsenbord) uit te zetten kan dan handig zijn.

Als er een totaaloplossing bestaat zou dit ideaal zijn, dit mag dan iets zijn wat alleen ondersteund wordt door Windows omdat dit voornamelijk gebruikt wordt. Er dient tevens een vergelijking gemaakt te worden van freeware en betaalde oplossingen.

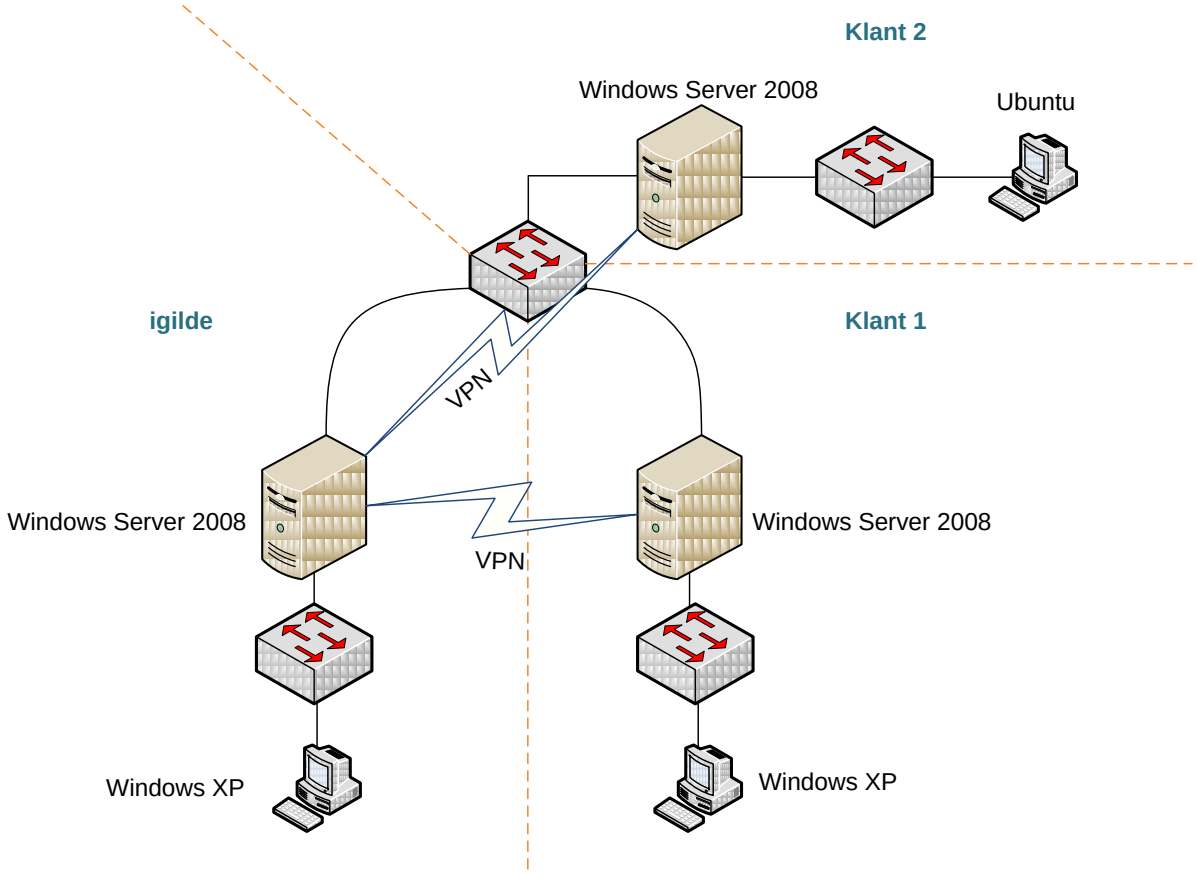
4.5 Ongewenste situatie

Tijdens de interviews is er ook een vraag gesteld over oplossingen met een werking vergelijkbaar met LogMeIn (http://www.logmein.com). Dit is een oplossing waarbij er handmatig op elke te beheren computer een programma geïnstalleerd moet worden die verbinding maakt met een server op het internet. Door in te loggen op de website zijn de aangemelde computers zichtbaar en kunnen deze overgenomen worden. Omdat hier onder andere een derde partij aan te pas komt waar geen invloed op uitgeoefend kan worden wil igilde dit niet als oplossing hebben.

5 Virtuele testomgeving

Om gedurende het project oplossingen te kunnen testen is er een virtuele testomgeving opgezet gebaseerd op het productienetwerk van igilde en de VPN verbindingen naar de klanten.

Een overzichtstekening van deze testomgeving is te zien in figuur 4:



Figuur 4: Netwerktekening virtuele testomgeving

Het gaat hierbij om drie netwerken voorzien van één Windows 2008 server en één Windows XP of Ubuntu cliënt. Één van deze netwerken stelt het netwerk van igilde voor en de andere twee stellen klantnetwerken voor. De servers hebben twee netwerk interfaces, één die de verbinding met het internet simuleert en één die aan het interne netwerk gekoppeld zit. De servers van de klanten verzorgen een VPN verbinding met de server van igilde die verkeer tussen de netwerken mogelijk maakt. Op deze manier kan vanaf één van de netwerken remote beheer naar het andere netwerk getest worden. Door het verbreken van de VPN verbindingen kunnen testen uitgevoerd worden voor het beheren van klanten zonder VPN verbinding.

De handleiding die gebruikt is als naslagwerk voor het opzetten van de testomgeving staat vermeld in de bronvermelding.

6 Mogelijkheden

Nadat alles in kaart gebracht is, is het brainstormen begonnen over wat er mogelijk is. Te beginnen met de veiligheid van het remote beheer. igilde maakt al gebruik van VPN verbindingen waardoor het verkeer al versleuteld wordt. Maar de beveiliging van de nieuwe situatie moet ook zeker voldoende beveiligd zijn om het kwaadwillende zo moeilijk mogelijk te maken. Hiervoor is gekeken naar standaarden en certificeringen om de veiligheid te kunnen beoordelen.

Daarna is er een uitgebreid onderzoek gedaan naar beschikbare software pakketten die gebruikt kunnen worden en tevens ook getest zijn. Deze zijn op bepaalde punten beoordeeld en hier is een score uitgekomen. Voor de drie hoogst scorende pakketten is een scenario geschreven om dit te kunnen gebruiken voor de klanten van igilde.

Het onderzoek is uiteindelijk afgesloten met de drie oplossingsscenario's.

6.1 Veiligheid

Er zijn een aantal aspecten onderzocht omtrent de veiligheid van remote beheer. Hierbij zijn de onderdelen FIPS en FCAPS naar voren gekomen die in de komende paragrafen behandeld zijn. Dit zijn essentiële onderwerpen voor keuzes die later in het project gemaakt zijn.

6.1.1 FIPS 140-2 standaard

De FIPS, Federal Information Processing Standard 140-2, is een computer beveiligingsstandaard van de Amerikaanse regering die gebruikt wordt voor het accrediteren van cryptografische modules. De originele Engelse titel is: *Security Requirements for Cryptographic Modules*. Deze standaard is gepubliceerd op 25 mei 2001.

Het nationale instituut voor standaarden en technologieën (Engels: National Institute of Standards and Technology (NIST)) ontwikkelde de FIPS 140 serie om de vereisten en standaarden van cryptografische soft en hardware modules te kunnen coördineren. De cryptografische modules zijn ontwikkeld door open source communities voor het gebruik bij de Amerikaanse regering en andere industrieën (zoals financiële en medische instellingen) die gevoelige ongeclassificeerde informatie verzamelen, opslaan, versturen en delen.

FIPS 140-2, wat staat voor de tweede versie van FIPS 140, bestaat uit vier beveiligingsniveaus met de eenvoudige benaming: "Niveau 1" tot "Niveau 4".

De uitleg van deze niveaus staan in bijlage 5.

6.1.2 FCAPS

FCAPS is het ISO telecommunicatie management model en framework voor netwerk management. FCAPS staat voor: *Fault, Configuration, Accounting, Performance en Security* wat de management categorieën zijn waar het ISO model de netwerk taken definieert. In organisaties waar niet gefactureerd wordt, wordt *"Accounting"* vaak vervangen door *"Administration"*.

FCAPS past in het straatje van dit project omdat het over computer management gaat en het informatie geeft over waar het beheren van netwerken aan moet voldoen. Daarom is hier een korte uitleg gegeven over FCAPS.

Gestructureerd beheer van de infrastructuur is een fundamentele eis. Veel organisaties zijn afhankelijk van hun IT services en met name de beschikbaarheid en de kwaliteit. Hierdoor is het noodzakelijk dat problemen zo snel mogelijk opgemerkt en verholpen worden. De tijd die nodig is om het probleem te verhelpen (ook wel MTTP: Mean Time To Repair) moet daarom zo ver mogelijk teruggedrongen worden zodat de onbereikbaarheid nihil is. Omdat dit tot dataverlies kan leiden of er zelfs levens vanaf kunnen hangen.

Hieronder worden de vijf onderdelen van FCAPS toegelicht:

6.1.2.1 Fault management

Een fout(Engels: fault) is een gebeurtenis met negatieve effecten. Het doel van Fault management is om deze fouten te herkennen, te corrigeren en te loggen. Daarbij worden er analyses gedaan om netwerkfouten te kunnen voorspellen en continuïteit van het netwerk zo goed mogelijk te waarborgen. Dit kan gerealiseerd worden door het monitoren van verschillende aspecten in het netwerk voor ongewone gebeurtenissen.

Als zich een fout of gebeurtenis voordoet zullen één of meerdere netwerk componenten de netwerk beheerder een notificatie sturen. Deze notificatie is bedoeld om een handmatige of automatische actie in gang te zetten. Bijvoorbeeld: meer data verzamelen om te identificeren waar het probleem vandaan komt of het online brengen van back-up apparatuur.

Het loggen van fouten is ook een manier om statistieken te kunnen genereren en de beschikbaarheid van individuele componenten inzichtelijk te maken. Op die manier kunnen zwakker plekken worden opgemerkt die opgelost kunnen worden.

6.1.2.2 Configuration management

Het doel van configuration management bevat:

- Configuraties van netwerk componenten verzamelen en bewaren
- Configureren van netwerkcomponenten vereenvoudigen
- Veranderingen in de configuratie bijhouden

6.1.2.3 Accounting management

Het doel van accounting management is het verzamelen van verbruikstatistieken van de gebruikers. Deze gegevens worden gebruikt om te factureren of het doorvoeren van quota's.

Veelgebruikte voorbeelden van protocollen die gebruikt worden voor accounting zijn: Radius, Tacacs en Diameter.

In organisaties waar niet gefactureerd wordt, wordt accounting vervangen door administration. De doelen van administration is het configureren en verstrekken van gebruikersaccounts, wachtwoorden en permissies. Het verzorgen van back-up voorzieningen en data synchronisatie valt hier ook onder.

6.1.2.4 Performance management

Performance management zorgt er voor dat het netwerk wordt voorbereid op de toekomst en dat de efficiëntie van het huidige netwerk wordt bepaald.

Onder netwerk performance wordt verstaan: doorvoersnelheid, hoeveelheid dataverkeer, transport fouten en response tijden.

Door het analyseren van deze gegevens kan de "gezondheid" van het netwerk gemeten worden. Doormiddel van waarschuwingen kunnen problemen met de capaciteit en betrouwbaarheid geïdentificeerd worden voordat het de service negatief beïnvloed.

Deze waarschuwingen activeren een alarm en worden vervolgens afgehandeld door het "fault management" proces.

6.1.2.5 Security management

Security management wordt gebruikt voor het controleren van de toegang tot de verschillende componenten in het netwerk. Veiligheid wordt gecreëerd doormiddel van authenticatie en encryptie.

Bron: http://www.tech-faq.com/fcaps.shtml

6.2 Software

Na het bestuderen van een aantal veiligheidsaspecten is er onderzoek gedaan naar verschillende aanbieders van software voor het remote beheren van externe netwerken. In dit geval de netwerken van de klanten.

Dit onderzoek is begonnen met het maken van een lange lijst van pakketten die enigszins in aanmerking kwamen. Deze lijst is als volgt:

- Goverlan
- Numara Track-IT
- GoToAssist
- TechInLine
- Timbuktu
- Remotelyanywhere
- TeamViewer
- Nomachine
- mRemote
- Remobo
- SimpleGateway
- Bomgar
- SmartCode VNC Manager
- Rhub
- Remote desktop manager
- Dameware NT Utilities

Deze pakketten zijn één voor één onderzocht op hun functionaliteiten waarbij er al een aantal afvielen. Zo is er een korte lijst ontstaan met de overgebleven pakketten die aan de meeste of alle eisen voldoen. Van deze pakketten zijn beschrijvingen gemaakt die in de volgende paragrafen te lezen zijn. Aan het eind hiervan is alles in een aantal kruistabellen gezet waarin de verschillende pakketten met elkaar zijn vergeleken. Hier is een score uitgekomen en een top drie bepaald. De pakketen uit deze top drie zijn gebruikt voor de verschillende oplossingsscenario's.

De pakketten die afgevallen zijn:

Pakket	Afgevallen omdat
Numara Track-IT	Bleek geen interesse te hebben in samenwerking. Meerdere malen om informatie gevraagd maar gaven hier geen gehoor aan.
GoToAssist TechInLine Remotelyanywhere TeamViewer Remobo	Vereist een server op het internet waarmee een verbinding wordt gemaakt. Vergelijkbaar met LogMeIn en is niet gewenst.
Timbuktu	Vereist een server op het internet waarmee een verbinding wordt gemaakt. Vergelijkbaar met LogMeIn en is niet gewenst. En er is geen duidelijke informatie over het pakket. Geen documentatie en de configuratie ging heel moeizaam.
NoMachine	Dit bleek een applicatie te zijn voor het centraal virtualiseren van desktop computers.
Rhub	Rhub is opgezet voor web conferences. Het bedienen van een computer door meerdere mensen. Niet bedoeld om support mee te leveren, is tevens een web applicatie wat igilde niet wil.
Remote desktop manager	Dit is een programma dat verschillende technieken omtrent remote beheer bevat. Echter geen mogelijkheid tot het vragen van toestemming aan de gebruiker van de remote computer, wat igilde als eis heeft gesteld.

Tabel 2: Afgevallen pakketten

De overgebleven pakketten zijn op een aantal van te voren gedefinieerde punten getest. Deze punten zijn tot stand gekomen tijdens het opzetten van de opdracht en tijdens de interviews. In tabel 3 zijn deze punten benoemd en toegelicht.

1.	Geschikt voor?	Is deze oplossing geschikt voor Windows systemen, voor Linux systemen, voor web based apparaten of Cisco apparatuur (telnet). Het is noodzakelijk om te weten of het pakket geschikt is voor het beheren van de apparaten die igilde en haar klanten gebruiken.
2.	Verbinden via RDP mogelijk?	Is het mogelijk om een verbinding op te zetten met het RDP protocol. Ook wel Remote desktop. Omdat het handig kan zijn om toch deze mogelijkheid te hebben is deze meegenomen in de te testen punten.
3.	Geschikt voor 32 bits of 64 systemen	Is de software geschikt voor 32 bits, 64 bits of beide Omdat igilde gebruik maakt van 32 en 64 bits systemen is het vereist om te weten of het programma geschikt is voor beide systemen.
4.	Moet de gebruiker toestemming geven om remote beheer toe te staan?	Als de gebruiker ingelogd is en de beheerder wil verbinding maken met de computer van de gebruiker, krijgt deze dan een bericht waarin toestemming gevraagd wordt. Om vertrouwen bij de klant op te bouwen dat het niet zo maar mogelijk is om op de computer in te kunnen loggen is een functie om de gebruiker via een scherm om toestemming te vragen erg handig.
5.	Is het mogelijk om bij afwezigheid van de klant, toch verbinding te maken?	Wanneer er niemand ingelogd is, of als de pc vergrendeld is, kan er dan wel zonder toestemming ingelogd worden? Als de gebruiker afwezig is kan deze geen toestemming geven. Erg lastig om groot onderhoud te kunnen plegen waar de gebruiker juist niet bij moet zijn. In een dergelijk geval moet het toch mogelijk zijn om zonder bijkomst van de gebruiker de computer over te nemen. Bijvoorbeeld doormiddel van een time-out.
6.	Is er server software nodig?	Is het nodig om op de computer van de beheerder software te installeren om verbinding te maken met de computer van de klant? Het is goed om te weten of de beheerders software moeten installeren om verbinding te maken met de computers. Als dat het geval is kan alleen beheer uitgevoerd worden vanaf de computer van de beheerder zelf of waar de software op geïnstalleerd is.
7.	Is er aparte cliënt software nodig?	Is het nodig om op de computers van de klanten software te installeren om verbinding te kunnen maken. Dit is nodig om te kunnen bepalen of er op de computers van de gebruikers van te voren software geïnstalleerd moet worden.
8.	Is deze distribueerbaar?	Als er cliënt software nodig is, kan deze eenvoudig gedistribueerd worden? Als dat het geval is, is het mogelijk om deze software van afstand te installeren of bijvoorbeeld automatisch geïnstalleerd kan worden vanaf hun server. Zodat het niet nodig om op locatie te komen om een computer klaar te maken voor remote beheer.
9.	Heeft het extra mogelijkheden dan alleen remote desktop?	Zijn er meer mogelijkheden dan alleen het overnemen van het scherm? Een extra toevoeging kan zijn of het programma extra functionaliteiten heeft wat de eenvoud van remote beheren bevorderd.
10.	Windows authenticatie?	Ondersteunt het programma Windows authenticatie? Om wachtwoordbeheer centraal te houden en de mogelijkheid te hebben om eenvoudig als beheerder in te kunnen loggen op het systeem is het vereist dat Windows authenticatie wordt ondersteund

11.	Is het wachtwoord van de klant nodig?	Is het nodig om het wachtwoord van de gebruiker te weten als er ondersteuning geboden wordt? Moet de gebruiker zijn wachtwoord aan de beheerder vertellen zodat deze zijn werk uit kan voeren? Omdat igilde niet meer de wachtwoorden aan haar gebruikers wil vragen moet het mogelijk zijn om met een beheerderwachtwoord in te loggen.
12.	Kunnen alleen beheerders inloggen?	Kunnen alleen gebruikers met administrator rechten inloggen om ondersteuning te bieden? Met andere woorden: kunnen er verschillende niveaus van rechten toegepast worden? Om een rechtenstructuur mogelijk te maken dat niet iedereen toegang heeft tot de beheersmogelijkheden i het noodzakelijk om te weten of deze functie aanwezig is.
13.	Is het BIOS van de remote computer configureerbaar?	Nieuwe technologieën maken het mogelijk om het BIOS van computers via het netwerk toegankelijk te maken zodat als het opstarten of afsluiten van de computer niet lukt deze bijvoorbeeld opnieuw aan en uitgezet kan worden. Een veelvoorkomend probleem is dat het besturingssysteem van de remote computer faalt. In dat geval biedt de huidige techniek de mogelijkheid om de computer aan en uit te schakelen van afstand. Dit is een eventuele goede toevoeging voor igilde.
14.	Is het freeware?	Is het gratis te gebruiken of zijn er licentiekosten aan verbonden? Kosten zijn een essentieel belang in het maken van keuzes, daarom worden de kosten van het aanschaffen en gebruik van de software vernoemd.
15.	Compatible met een opstaphost?	Is het mogelijk om de oplossing te gebruiken in combinatie met een opstaphost die de toegang tot het netwerk van de klant verleend. Omdat igilde een opstaphost een mooie optie vindt is het goed om te weten of dit mogelijk is met het pakket.
16.	Is het mogelijk om het externe toetsenbord + muis uit te schakelen.	Het toetsenbord en de muis van de externe computer kunnen uitgeschakeld worden om eventuele problemen te voorkomen dat langslopende mensen die een muis zien bewegen gaan tegenwerken. Met de mogelijkheid dat klanten mee kunnen kijken tijdens het beheer kan het gebeuren dat de klant zijn muis blijft bewegen of het toetsenbord blijft gebruiken. Een optie om deze invoerapparaten tijdelijk uit te schakelen voorkomt deze problemen.
17.	Wat is het bandbreedte verbruik	Hoeveel verkeer genereert het remote beheren van de computer? Omdat igilde de mogelijkheid in acht wil houden om beheer mogelijk te maken via mobiel internet moet het bandbreedte verbruik zo laag mogelijk zijn.
18.	FIPS Niveau	Op welk FIPS Niveau bevindt het programma zich? (Zie paragraaf 6.1.1) FIPS is een certificering voor de veiligheid van het pakket. Erg belangrijk om te weten of het programma deze certificering heeft gekregen en op welk niveau.

Tabel 3: De onderzochte elementen

De software pakketten die de eerste selectie hebben doorstaan zijn:

- DameWare Mini Remote
- DameWare NT Utilities (inclusief Mini Remote)
- Goverlan Remote Control
- Radmin
- mRemote
- Simple gateway
- smartCode VNC manager
- Bomgar
- secureCRT
- Putty connection manager

De testresultaten van deze pakketten zijn in onderstaande paragrafen beschreven.

6.2.1 Dameware Mini Remote

Dameware Mini Remote is een simpele manier van het remote beheren van Windows systemen. Het gaat hierbij om een simpele interface waarin eerdere connecties opgeslagen kunnen worden. Voordat echt verbinding gemaakt wordt met de pc van de klant moet er een service geïnstalleerd worden. Dit kan eenmalig automatisch gebeuren zodra verbinding gemaakt wordt, hier zal automatisch om gevraagd worden. Voor een groot netwerk kan er via een ingebouwde MSI builder een automatisch installatie bestand aangemaakt worden die via de Group Policy van het Windows domein verspreidt wordt. DameWare Mini Remote maakt gebruik van TCP port 6129 die toegestaan moet worden in de firewall. DameWare heeft wat extra features in het pakket zitten zoals:

- Uitschakelen van extern toetsenbord en muis
- Alleen meekijken met de klant
- Verbinden via het RDP protocol

Een sterk punt van DameWare is dat bij installatie van de cliënt software gekozen kan worden voor de functie dat de gebruiker toestemming moet geven voor het remote beheer en een melding krijgt met door wie je geholpen wordt. Hierbij is het niet nodig om het wachtwoord van de gebruiker te weten. Met een beheerderaccount is het mogelijk om in te loggen op de actieve sessie van de gebruiker. Mocht de computer vergrendeld of nog niet ingelogd zijn dan is het mogelijk om zonder toestemming van de computer over te nemen. Voor servers geld dat deze functie niet aangezet wordt omdat er niet iemand achter een server zit te werken die toestemming kan geven. Toegang tot de server moet er altijd zijn, dan wordt deze functie niet aangezet.

De grafische weergave tijdens het beheer kan teruggeschroefd worden naar 8 bit waardoor het gemiddelde bandbreedte verbruik rond de 70 kbps* ligt.

DameWare Mini Remote is niet gratis en hanteert een “per user” licentie. Per gebruiker dient er één licentie aanwezig te zijn. Of de gebruiker die de licentie in handen heeft nou op zijn thuis computer werkt of op het werk maakt geen verschil net als het aantal remote computers. Zijn er meerdere die op één computer werken met het programma dan moet er voor elke gebruiker een licentie aangeschaft worden.

De licentiekosten zijn volgens onderstaande tabel:

1 User Licentie	$90.00
3 User Licentie	$259.00
5 User Licentie	$389.00
10 User Licentie	$719.00
25 User Licentie	$1729.00
50 User Licentie	$3149.00

Bron: http://www.dameware.com/products/

6.2.2 DameWare NT Utilities(DNTU)

NT Utilities is een verzameling management tools in één gecentraliseerde interface. DNTU bevat een Active Directory(AD) Browser die het ontvangen, doorzoeken en filteren van AD objecten mogelijk maakt. Zoals: Organizational Units, Containers, Gebruikers, Groepen, Contacten, Computers en gedeelde mappen.

DNTU ondersteunt het beheren van Domeinen, werkstations, Disk Drives, Event Logs, Lokale Groepen, Globale groepen, Domain members, Openstaande bestanden, Printers, Processen, Register, Services, sessies, Shares, Afsluiten/Opnieuw opstarten, Software, Terminal Services/RDP, Users, Wake-on-Lan, en nog veel meer.

DNTU bevat ook de applicatie: Mini Remote zoals in de vorige paragraaf vermeld is.

DNTU is erg handig in combinatie met een opstaphost binnen het netwerk van de klant. Er kan gemakkelijk gebladderd worden tussen de computers die aangemeld zijn op het domein. Daarna kan er gekozen worden welke acties ondernomen moeten worden met die computer.

Het bandbreedte verbruik van DNTU ligt rond de 50 kbps*.

DameWare maakt gebruik van de BSAFE Crypto-C Micro Edition cryptografie module die voldoet aan alle Level 1 vereisten van de FIPS 140-2 standaard (Zie paragraaf 6.1.1).

DNTU is niet gratis en hanteert een “per user” licentie. Per gebruiker dient er één licentie aanwezig te zijn. Of de gebruiker die de licentie in handen heeft nou op zijn thuis computer werkt of op het werk maakt geen verschil net als het aantal remote computers. Zijn er meerdere die op één computer werken met het programma dan moet er voor elke gebruiker een licentie aangeschaft worden.

De licentiekosten zijn volgens onderstaande tabel:

1 User Licentie	$289.00
3 User Licentie	$829.00
5 User Licentie	$1229.00
10 User Licentie	$2319.00
25 User Licentie	$5569.00
50 User Licentie	$10119.00

Bron: http://www.dameware.com/products/

6.2.3 Goverlan

Goverlan heeft net als DameWare een variant waar ook een aantal beheeropties bijzitten en een variant waar alleen remote desktop mee uitgevoerd kan worden. Goverlan Remote Control kan verbinding maken met RDP en VNC cliënts maar heeft ook een eigen agent waarmee verbinding gemaakt kan worden. Bij Windows machines wordt er bij het verbinden gevraagd of deze agent geïnstalleerd moet worden. Na het invullen van credentials die gemachtigd zijn zal dit gebeuren en kan het scherm overgenomen worden. Deze agent werkt over een enkele TCP/IP port die in de firewall moet worden toegestaan. Distribueren van de agent is niet nodig. Linux machines kunnen beheerd worden door een VNC server te installeren waarmee verbinding gemaakt kan worden. Goverlan bied geen mogelijkheid om via SSH verbinding te maken. Er kan wel verbinding gemaakt worden met Citrix machines door het installeren van een Citrix cliënt.

Met de Goverlan Management console kan er door de Active Directory gebladerd worden om een overzicht te krijgen welke computers zich in het netwerk bevinden en welke online/offline zijn.

Goverlan biedt niet de mogelijkheid om de gebruiker om toestemming te vragen, wel krijgt de gebruiker een bericht waarbij gemeld word wie er verbinding gemaakt heeft en krijgt 10 seconden de mogelijkheid om de verbinding te verbreken. Dit geld overigens alleen voor de Goverlan agent, bij het verbinden met een VNC server gelden de VNC opties.

Het minimale bandbreedte verbruik van Goverlan is 100 kbps* en de licentiekosten zijn als volgt:

	Prijs per gebruiker	1 jaar updates
Goverlan	$699	$199
Goverlan Remote Control	$229	$89

Bron: http://www.pjtec.com

6.2.4 Radmin

Radmin is op zijn beurt een eenvoudige tool om externe Windows systemen over te nemen. Radmin heeft niet de mogelijkheid om door de Active Directory te bladeren, waardoor verbindingen handmatig toegevoegd moeten worden. Deze zijn wel te ordenen doormiddel van submappen. Radmin kan alleen verbinding maken met de cliënt software van Radmin die eenvoudig te distribueren is doormiddel van een MSI creator waarna het MSI bestand via de Group Policy verspreid kan worden. Zodra de server geïnstalleerd en gestart is kan er onder anderen gekozen worden of de klant toestemming moet geven. Als deze optie gekozen wordt moet er daarna opgegeven worden of er na een time-out toch toestemming verleend wordt of dat de toestemming dan geweigerd wordt. Een lastig punt is dat zodra de klant de computer niet inlogt of vergrendeld is deze toestemming nog steeds vereist, dus als er voor gekozen is om na de time-out toegang te weigeren kan er geen verbinding gemaakt worden tot er door iemand op “Ja” geklikt wordt. Het is

daarom een aanrader om na een time-out toch toegang te laten verlenen en de klant de mogelijkheid te geven om toegang eventueel te weigeren.

Voor de beheerder moet ook een programma geïnstalleerd worden wat ook via Group Policy gedistribueerd kan worden.

Daarbij is er ook ondersteuning voor Intel AMT (Active Management System). Waarbij het mogelijk is om computers waarbij het besturingssysteem weigert, toch opnieuw op te starten, uit te zetten of op te starten van een cd-rom of netwerkbron. Ook kan hiermee het bios van afstand geconfigureerd worden. Uiteraard moet het moederbord van de externe computer deze technologie ondersteunen.

Radmin werkt in een gecodeerde modus waarbij alle gegevens, schermafbeeldingen, muisbewegingen en toetsenbordsignalen gecodeerd worden met gebruik van een 256-bit AES sterke codering met willekeurig gegenereerde sleutels voor elke verbinding. Voor gebruikersverificatie kan Radmin Windows beveiliging met Active Directory en Kerberos-ondersteuning gebruiken, of de eigen beveiliging met afzonderlijke gebruikerstoestemming en beveiligde login/wachtwoord verificaties. Radmin beveiliging gebruikt sleuteluitwisseling op Diffie-Hellman basis met 2048-bit sleutelgrootte. Aanvullende IP-filters beperken toegang tot bepaalde hosts en netwerken.

Het gemiddelde bandbreedte verbruik van Radmin is 150 kbps* bij een 8 bits weergave. En Radmin kan een minimale weergave van 1 bit weergeven (zwart/wit).

Het licentiemodel is “per remote computer”. Als er 100 computers beheerd moeten worden, moeten deze elk een aparte licentie hebben. Er kan gekozen worden uit een standaard licentie, een volume licentie of een helpdesk licentie. De helpdesk licentie is interessant voor igilde, deze biedt goedkopere licenties voor het ondersteunen van klanten maar vereist het aanschaffen van minimaal 50 licenties. Voor het gebruik van minder licenties kunnen individuele standaard licenties gebruikt worden. De kosten zijn als volgt:

Licentie	**Geldig voor**	**Prijs, EUR(€)**
Standaard licentie	Enkele pc	€37,10
50 licentie pakket	Tot 50 pc’s	€1129,00
100 licentie pakket	Tot 100 pc’s	€1886,00
150 licentie pakket	Tot 150 pc’s	€2644,00
Volume licentie	Vanaf 200 pc’s	€16,70
Helpdesk licentie	Vanaf 50 pc’s	€25,00

Bron: http://www.radmin.com

6.2.5 mRemote

mRemote is een freeware programma voor het beheren van Windows machines, Linux machines, web enabled apparaten Citrix servers, routers en switches. mRemote maakt hierbij gebruik van VNC en RDP voor de Windows machines, putty voor de Linux machines en de routers en switches. Voor de web enabled apparaten wordt internet explorer gebruikt.

mRemote is een console waarin handmatig verbindingen toegevoegd kunnen worden. Bij het toevoegen wordt er een naam gegeven aan de verbinding en aangegeven om welke verbinding het gaat: RDP, VNC, telnet, SSH(voor Linux), http(s) of ICA(Citrix). Binnen de console van mRemote wordt er vervolgens met het bijbehorende programma een verbinding opgezet. De RDP functie is handig voor servers maar niet voor cliënts, zoals in de huidige situatie is beschreven. mRemote bied de mogelijkheid om verbinding te maken met een gratis VNC server. VNC moet dan wel op de externe computer geïnstalleerd worden. Het nadeel van de gratis versie van VNC server is dat er geen sterke encryptie gebruikt wordt en Windows authenticatie niet mogelijk is. Hierdoor moet er verbinding gemaakt worden met een enkel statisch wachtwoord. Door dit wachtwoord alleen bekend te maken bij beheerders zorg je dat deze niet voor iedereen toegankelijk is.

De slechte encryptie wordt grotendeels gecompenseerd door de IPsec VPN verbinding tussen de klant en igilde waardoor de data die over het internet gaat alsnog versleuteld wordt. Op beide interne netwerken is dit niet meer van toepassing. Dit geld ook voor het slecht beveiligde telnet.

Alleen bij VNC is het mogelijk om deze zo in te stellen dat de klant toestemming moet geven voor de verbinding, bij afwezigheid van de gebruiker is verbinden onmogelijk. De bandbreedte per applicatie is:

VNC	30 kbps* (bij 64 kleuren)
SSH/telnet	15 kbps*
http	80 kbps*
RDP	60 kbps* (bij 256 kleuren)
Gemiddeld	50 kbps

Bron: http://www.mremote.org

6.2.6 simpleGateway

SimpleGateway is een op Java gebaseerd multi platform remote desktop applicatie. SimpleGateway hanteert hetzelfde principe als logmein.com waarbij er een centrale server is waarop de cliënts zich aanmelden. Door het inloggen op deze server kunnen de cliënts beheerd worden. Het verschil van simpleGateway is dat deze centrale server geïnstalleerd wordt op een server in het lokale netwerk (kan ook op internet). Op de cliënts wordt handmatig de cliëntsoftware geïnstalleerd en de server opgegeven waar deze cliënt zich aan moet melden. Het is mogelijk om meerdere servers op te geven. In de server console, in de vorm van een website, verschijnt deze cliënt in een lijst waarna de sessie opgezet kan worden. Deze lijst is niet te ordenen in mappen, het is één lange lijst die doormiddel van een filter doorzocht kan worden.

Het inloggen op de website gebeurd standaard via een eigen gebruikersdatabase die in een XML bestand staat maar kan ook via een LDAP server afgehandeld worden. Door de authenticatie zorg je ervoor dat alleen gemachtigde in kunnen loggen op de website.

Zowel de server als de cliënt zijn geschikt voor 32 bits en 64 bits Windows, Grafische Linux en Mac OS desktops/servers. Het ondersteunt geen SSH, telnet of RDP.

Bij simpleGateway is het alleen mogelijk om de gebruiker op de hoogte te brengen van wie er een verbinding heeft gemaakt. Er kan niet om toestemming gevraagd worden.

SimpleGateway garandeert een veilige verbinding vanaf de remote computer en de computer van de beheerder doormiddel van een 448 bit asymmetrisch SSL protocol, zelfs de simpleGateway server kan de datastroom niet afluisteren. Daarbij gebruikt simpleGateway de laatste “ObjectSign Code” certificaten van GlobalSign om er zeker van te zijn dat de software legitiem is en van de juiste leverancier komt.

Bij minimale weergave (zwart/wit) gebruikt simpleGateway 90 kbps*.

De licentie geld als volgt:

Het aantal licenties dat aangeschaft wordt geld voor het aantal sessies die tegelijk uitgevoerd mogen worden. Als er tien computers tegelijk beheerd moet worden zijn er tien licenties vereist. Ongeacht het aantal aangemelde computers en het aantal beheerders. De eenmalige kosten van deze licenties staan in onderstaande tabel:

Licentie	Aantal computers	Beheerders	Actieve sessies	Prijs
SimpleGateway 1	Onbeperkt	Onbeperkt	1	$265
SimpleGateway 2	Onbeperkt	Onbeperkt	2	$445
SimpleGateway 3	Onbeperkt	Onbeperkt	3	$670
SimpleGateway 4	Onbeperkt	Onbeperkt	4	$895
SimpleGateway 5	Onbeperkt	Onbeperkt	5	$895
SimpleGateway 6	Onbeperkt	Onbeperkt	6	$1075
SimpleGateway 7	Onbeperkt	Onbeperkt	7	$1255
SimpleGateway 8	Onbeperkt	Onbeperkt	8	$1435
SimpleGateway 9	Onbeperkt	Onbeperkt	9	$1615
SimpleGateway 10	Onbeperkt	Onbeperkt	10	$1345

Bron: http://www.simple-help.com

6.2.7 smartCode VNC manager Enterprise

De naam VNC manager zegt al wel een beetje wat het programma doet. Het programma beheert VNC connecties. Vanuit deze console kan simpel een verbinding opgezet worden naar een VNC cliënt, maar ook een RDP, SSH, Telnet of Hyper-V cliënt. VNC is geschikt voor Windows en Linux machines zowel 32 als 64 bit.

De VNC manager biedt verschillende tools om het netwerk te scannen naar beschikbare computers. Zo ook een Active Directory browser. Hierin zijn alle computers die zijn aangemeld bij het domein te zien.

Omdat VNC manager onder andere gebruik maakt van ultraVNC is het mogelijk om na een time-out toch toestemming te krijgen. De authenticatie kan ook via Windows authenticatie lopen waardoor het wachtwoord van de klant niet nodig is.

VNC manager biedt niet veel extra's. Wel zijn er een aantal plug-ins waarmee standaard computerbeheer uitgevoerd kan worden(apparaatbeheer, Event logs, Printer beheer, services, shares etc.) binnen de VNC manager en niet op het scherm van de klant verschijnt.

Een extra feature is dat er thumbnails bekeken kunnen worden van alle daarvoor aangemelde computers. Zo kan er snel een overzicht verkregen worden van wat er op de computers gebeurd.

VNC manager heeft geen ingebouwde beveiliging maar vertrouwt op de veiligheid van de verschillende add-ons in het programma. UltraVNC is te gebruiken met een MSRC4 plug-in die goed is voor een 128 bits encryptie.

VNC manager is geen freeware en hanteert een "per user" licentie. Waarbij elke gebruiker een onbeperkt aantal machines mag beheren. De kosten hiervan zijn als volgt:

Licentie	**Aantal gebruikers**	**Kosten**	**Licentieduur**
Enkele gebruiker	1	$118,75	1
5 enkele gebruikers	5	$534,38	1
Bedrijfslicentie	Onbeperkt	$1600,00	1
Enkele gebruiker	1	$165,99	2
5 enkele gebruikers	5	$746,96	2
Enkele gebruiker	1	$296,31	Onbeperkt
5 enkele gebruikers	5	$1333,40	Onbeperkt
Bedrijfslicentie	Onbeperkt	$3000,00	Onbeperkt

6.2.8 Bomgar Remote Support

Bomgar is vergelijkbaar met simpleGateway. Bomgar is ook een multiplatform remote desktop oplossing met extra mogelijkheden ten opzichte van simpleGateway. Bomgar kan naast Windows, Linux en Mac computers ook Windows mobile en blackberry telefoons beheren. Om Bomgar te gebruiken moet er een “Bomgar Box” aangeschaft worden. Dit is de server waarop de beheerders inloggen om ondersteuning te bieden en klanten zich aanmelden om ondersteuning te krijgen.

Bomgar ondersteunt net als simpleGateway geen SSH, Telnet en RDP. Uiteraard is dit op te lossen doormiddel van een opstaphost. Eerst verbinding maken met een beheer server (bijvoorbeeld met Bomgar) en vanuit daar een SSH, Telnet of RDP sessie opzetten.

Bomgar vereist cliënt software om verbinding te maken met de server, een groot voordeel is: dat het niet nodig is om deze software te distribueren. Klanten kunnen naar een website surfen, die in de huidige website geïntegreerd kan worden, om daar een sessiecode in te vullen die ze ontvangen van de beheerder waarna de tijdelijke software gedownload wordt en de machine overgenomen kan worden. De beheerder kan ook een mail sturen naar de klant waarin een link zit waar de sessie code al in verwerkt zit, bij het klikken op deze link kan na bevestiging de computer overgenomen worden. Dit zijn acties waarbij er iemand achter de computer moet zitten om ondersteuning te bieden. Bomgar kan doormiddel van een “Jump” functie een computer ook pushen om verbinding te maken, dit kan uiteraard alleen als de beheerder in het bezit is van administrator credentials. Als dit op deze manier gebeurd kan er alsnog een optie meegegeven worden waarin op het externe scherm een melding verschijnt of beheer afgewezen moet worden en dat na 10 seconden automatisch toegang verleend wordt. De zogenoemde “Jump” software kan ook op een PC geïnstalleerd worden zodat deze continue aangemeld blijft op de BomgarBox en altijd toegankelijk is ongeacht in welk netwerk deze pc zich bevind.

“Jump” kent ook een optie die heet: “Jumppoint”. Dit wordt binnen een netwerksegment op een Windows machine geïnstalleerd en maakt het mogelijk om via die PC het netwerk te identificeren. Via die PC kunnen er jump sessies opgestart worden met de rest van het netwerk zonder in te loggen op de “jumpoint”. In de beheerderconsole wordt het jumpoint geselecteerd waarna uit de andere pc’s in het netwerk gekozen kan worden. Zoals misschien al duidelijk is werkt de jump functie alleen op Windows machines.

Een mooie functie van Bomgar is het delen of escaleren van remote sessies. Als er meer beheerders ingelogd zijn op Bomgar is het mogelijk om iemand anders uit te nodigen op een remote sessie als er hulp nodig is. De pc wordt dan tijdelijk door 2 beheerders beheerd die onderling kunnen overleggen doormiddel van de chat. Ook kan een sessie verplaatst(geëscaleerd) worden naar een andere beheerder. Het verschil is dat de eerste sessie wordt beëindigd.

Bomgar heeft extra functies, zoals een dashboard waar onder andere naar het CPU, geheugen en harde schijf gebruik gekeken kan worden, ook kan er eenvoudig gechat worden met de gebruiker. Ook heeft Bomgar ingebouwde failover functies waarbij bij uitval van een server een andere gesynchroniseerde server het werk over kan nemen.

Bomgar ondersteunt verschillende authenticatie mogelijkheden zoals Radius, LDAP en Active Directory. Dit zijn credentials die nodig zijn om als beheerder in te loggen op de server. De klant heeft alleen een sessiecode nodig.

Om de verbinding tussen de beheerder en de klant te beveiligen wordt een 256 bits AES SSL encryptie gebruikt. Bomgar kan veiligheid garanderen doordat Symantec deze geverifieerd heeft. Bomgars beveiliging opereert op FIPS Niveau 2. (Zie paragraaf 6.1.1)

Om conflicten te voorkomen worden de remote sessies als flash filmpjes opgeslagen zodat deze terug te zien zijn. In deze filmpjes is te zien wie op de momenten het toetsenbord en de muis bestuurden zodat bij onduidelijkheid acties niet aan een ander te verwijten zijn. De filmpjes kunnen ook gebruikt worden voor kwaliteitscontrole. De filmpjes worden op een extern media opgeslagen.

Een software development kit(SDK) maakt het mogelijk om eenvoudige aanpassingen aan het systeem te maken.

Het data verbruik van Bomgar is maar 50 kbps *.

Bomgar is niet gratis en hanteert een principe waarbij de hardware en de licenties eenmalig worden aangeschaft. Het maakt niet uit hoeveel gebruikers in het systeem staan, het gaat om het aantal gebruikers die tegelijkertijd ingelogd kunnen zijn. In overleg met een sales manager van Bomgar is geconcludeerd dat de zogenoemde B200 Bomgar Box met standaard licenties een geschikte oplossing zal zijn voor igilde. Bomgar biedt optioneel(eerste jaar verplicht) onderhoud aan op haar producten, dit bestaat uit: Gratis updates naar nieuwe versie, bij hardware problemen gratis vervanging en een tijdelijke cold stand-by server gehost door Bomgar en onbeperkt technische support van de helpdesk.

Bomgar heeft een offerte gemaakt aan de hand van de volgende vastgestelde gegevens:

- B200 Bomgar Box (Bomgar server)
- 5 Standaard licenties
- Onderhoudscontract

Dit komt op een bedrag van: $18149 eenmalige kosten. Extra licenties en hardware zijn altijd apart aan te schaffen.

Bron: www.bomgar.com

6.2.9 SecureCRT

SecureCRT is een telnet/SSH connection manager om vanaf Windows computers Telnet/SSH servers te beheren. In het geval van igilde is het onder andere mogelijk om Linux servers en Cisco apparatuur te beheren. De verbindingen met deze apparatuur kunnen opgeslagen worden, inclusief de wachtwoorden, wat uiteraard niet aangeraden wordt. Via tabs kunnen meerdere sessies tegelijk geopend en geordend worden waardoor je overzichtelijk aan meerdere apparaten tegelijk kan werken.

SecureCRT ondersteunt het SSH2 protocol met als authenticatie mogelijkheden: RSA, DSA, X.509 en Kerberos in combinatie met een 2048 bits encryptie(AES, TwoFish, BlowFish, 3DES en RC4).

Een handige functie is dat er “key mappings” ingesteld kunnen worden. Er kunnen commando’s aan toetsenbordcombinaties gekoppeld worden. Dit is handig als je bepaalde commando’s vaak gebruikt. En daarbij houd SecureCRT een geschiedenis van 128.000 lijnen bij die gemakkelijk terug te halen zijn. Ook kan er een chat-window geopend worden waarin meerdere commando’s gezet kunnen worden die vervolgens tegelijk naar de server worden verzonden.

Dan is het ook nog eens heel eenvoudig om commando’s te kopiëren en te plakken in en vanuit de SecureCRT console.

In combinatie met SecureFX, een SFTP programma wordt het ook heel eenvoudig om de bestanden op de SSH server te beheren. SecureCRT en SecureFX hebben de mogelijkheid om inloggegevens te cashen waardoor als er geschakeld wordt tussen beide programma’s het niet nodig is om opnieuw in te loggen.

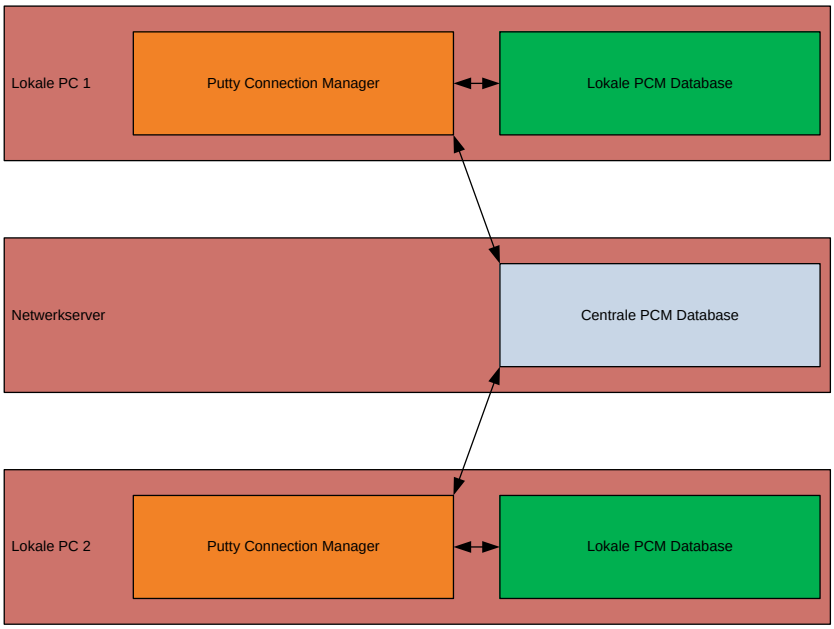
Beide programma’s zijn geen freeware en hanteren een “per user” licentie, de kosten staan hieronder:

Product	**Aantal**	**Prijs met 3 jaar updates**	**Prijs met 1 jaar updates**
SecureCRT	1	$139,00	$99,00
	2 – 9	$133,00	$95,00
	10 – 24	$129,00	$92,00
	25 – 49	$117,00	$88,00
	50 - 99	$110,00	$83,00
SecureCRT + SecureFX	1	$179,00	$129,00
	2 – 9	$175,00	$125,00
	10 – 24	$169,00	$121,00
	25 – 49	$157,00	$118,00
	50 - 99	$146,00	$110,00

Bron: http://www.vandyke.com

6.2.10 Putty Connection Manager

Putty Connection Manager(Verder afgekord als: PCM) is te vergelijken met SecureCRT alleen heeft het geen opties om bestanden op de remote SSH server te beheren. De naam zegt het al een beetje, het is een connection manager voor de SSH cliënt: “Putty”. Putty moet ook apart gedownload worden. Vervolgens wordt er een database bestand aangemaakt die op een share geplaatst kan worden. In deze database worden de connecties opgeslagen die ingevoerd zijn. Het voordeel hiervan is dat deze ook door andere gebruikers uitgelezen kan worden. Niet iedereen hoeft zijn eigen persoonlijke database samen te stellen, hoewel je dat ook in combinatie kan gebruiken. Er kunnen meerdere databases aan het programma gekoppeld worden, waarvan er één bijvoorbeeld van het netwerk is waar iedereen bij kan en één een persoonlijke database is waar connecties in staan die alleen door diegene gebruikt worden.



PCM heeft een mooie ingebouwde Window manager waardoor je de openstaande connecties heel mooi en netjes kan ordenen zonder ze zelf op maat te maken. Doormiddel van slepen wordt een scherm als extra tabblad, naast, boven of onder het huidige scherm weergegeven. De al openstaande schermen worden automatisch aangepast aan de beschikbare ruimte waardoor het niet nodig is om onnodig te schuiven met openstaande schermen. Dit werkt heel overzichtelijk.

Putty maakt gebruik van AES encryptie en RSA.

PCM is freeware en gratis te gebruiken.

Bron: http://puttycm.free.fr/cms/

**Bandbreedte verbruik is gemeten met de laagst mogelijke kleurweergave tijdens het verslepen van een JPG plaatje ter grote van 100 kilobyte.*

6.3 Overzichten

Nadat de pakketten de test hebben ondergaan zijn de resultaten in een kruistabel gezet om een overzicht te krijgen. Deze tabel ziet er als volgt uit:

	Windows	Linux	Web enabled devices	SSH	Telnet	RDP Mogelijk?	X86	X64	Toestemming geven mogelijk?	Server Software?	Client software?	Client software distribueerbaar?	Extra mogelijkheden?	Windows authenticatie	Klantwachtwoord nodig?	Alleen toegankelijk voor beheerders?	Bios configureerbaar?	Freeware	Kosten	Extern toetsenbord/muis uitschakelen?	compatible met opstaphost?	Bandbreedteverbruik	FIPS Niveau
DameWare Mini Remote	x					x	x	x	x	x	x	x	x	x		x			+/- $90 per user	x		70 kb/sec	1
DameWare NT Utilities	x					x	x	x		x	x	x	x	x		x			+/- $289 per user	x		50 kb/sec	1
Goverlan Remote Control	x	x**				x	x	x		x	x	x		x		x			+/- $229 per user	x	x	100 kb/sec	
Radmin	x						x	x	x	x	x		x	x		x	x		+/- €25 per pc	x		150 kb/sec	
mRemote	x	x**	x	x	x	x	x	x	x***	x	x		x		x**	x		x	freeware	x		50 kb/sec	
simplegateway	x	x					x	x		x	x					x			+/- $265 per actieve sessie	x		90 kb/sec	
smartCode VNC manager	x	x			x	x	x	x	x	x	x	x	x	x		x			+/- $118,75	x		100 kb/sec	
Bomgar	x	x					x	x	x	x	x	x	x	x		x			+/- $18149,00		x	90 kb/sec	2
SecureCRT		x		x	x		x	x			x	x				x			+/- $139 per user	x		15 kb/sec	
Putty Connection Manager		x		x	x		x	x			x	x				x		x	freeware	x		15 kb/sec	
Remote Desktop	x					x	x	x	x					x		x				x		250 kb/sec	

** Via een apart te installeren VNC server
*** doormiddel van de VNC functie

Tabel 4: Overzicht van de functionaliteiten van alle pakketten

Uit tabel 4 kunnen een aantal conclusies getrokken worden:

- Een totaalpakket voor alle elementen is er niet
- mRemote voldoet aan vrijwel alle eisen maar is niet heel veilig en de authenticatie is minimaal
- Remote Desktop gebruikt ten opzichte van de andere veel bandbreedte
- Alle pakketten ondersteunen 32 en 64 bits systemen
- Alleen Bomgar en DameWare zijn FIPS 140-2 gecertificeerd
- DameWare is een applicatie die het beheer van Windows systemen vereenvoudigd en heeft veel extras.
- Putty Connection manager is een mooie applicatie voor het beheren van veel SSH servers maar kan verder niets
- Radmin is de enige die van afstand het bios kan beïnvloeden
- Bomgar heeft de hoogste score en is ook een goed werkbare applicatie maar biedt geen SSH, Telnet, RDP en is ten opzichte van de rest heel duur.
  (In de nieuwe versie van Bomgar is er wel SSH ondersteuning)

De kosten zoals ze in tabel 4 staan geven geen duidelijke weergave van de werkelijke kosten. Om die reden is er een duidelijker overzicht van de kosten gemaakt. Bij deze berekeningen is uitgegaan van vijf beheerders en 150 te beheren objecten over een tijdsbestek van één jaar. De gebruikte wisselkoers voor de omrekening van Dollar naar Euro is: $1 = € 1,48738

Het kosten overzicht is te vinden in bijlage 3.

6.4 Beoordeling

Als afsluiting van het onderzoek naar de verschillende pakketten zijn ze per punt beoordeeld. De boordeling heeft plaatsgevonden met een score van vijf niveaus (0 t/m 4) waarbij 4 de beste score is en 0 de slechtste score. De verschillende niveaus hebben volgens onderstaande tabel nog een benaming gekregen:

0	Ontbreekt
1	Aanwezig met gebreken
2	Aanwezig, niet speciaal
3	Aanwezig, enkele uitblinkers
4	Aanwezig, uitgebreid

De drie hoogst scorende pakketten zijn weergegeven in tabel 5, omdat de twee DameWare pakketten gelijk gescoord hebben en gelijkwaardig aan elkaar zijn, worden deze als één gezien en is DameWare NT Utilities als best geschikt gekozen omdat deze extra beheerfuncties heeft. Putty connection manager is een zeer eenvoudige manager voor het beheren van SSH servers. Omdat dit een freeware programma is zal deze, waar het handig is als advies aangeboden worden.

	Windows	Linux	Web enabled devices	SSH	Telnet	RDP Mogelijk?	X86	X64	Toestemming geven mogelijk?	Server Software?	Client Software?	Client software distribueerbaar?	Extra mogelijkheden?	Windows authenticatie	Klantwachtwoord nodig?	Bios configureerbaar?	Alleen toegankelijk voor beheerders?	Freeware	compatible met opstaphost?	Kosten	Extern toetsenbord/muis uitschakkelen?	Bandbreedteverbruik	FIPS Niveau	Totaal
Bomgar	**4**	**2**	**0**	**0**	**0**	**0**	**2**	**2**	**2**	**4**	**3**	**3**	**4**	**2**	**2**	**2**	**0**	**0**	**0**	**4**	**2**	**2**	**3**	**43**
DameWare NT Utilities	4	0	0	0	1	2	2	2	2	3	2	4	3	2	2	2	0	0	2	2	2	2	2	41
mRemote	2	1	2	2	2	2	2	2	1	2	2	1	0	1	1	2	0	4	4	2	1	3	0	39

Tabel 5: Scoretabel van de drie hoogst gescoorde pakketten

Scores zijn gebaseerd op persoonlijke ervaringen

De volledige tabel is weergegeven in bijlage 4.

Voor deze drie pakketten is in de komende hoofdstukken een oplossingsscenario geschreven.

7 Oplossingsscenario's

Na het afronden van de onderzoeken zijn voor de drie hoogst scorende pakketten een oplossingsscenario geschreven. Deze scenario's vormen een advies over hoe de pakketten in gebruik genomen kunnen worden. Dit is tevens het resultaat van het onderzoek.

De pakketten die door de selectie heen zijn gekomen zijn:

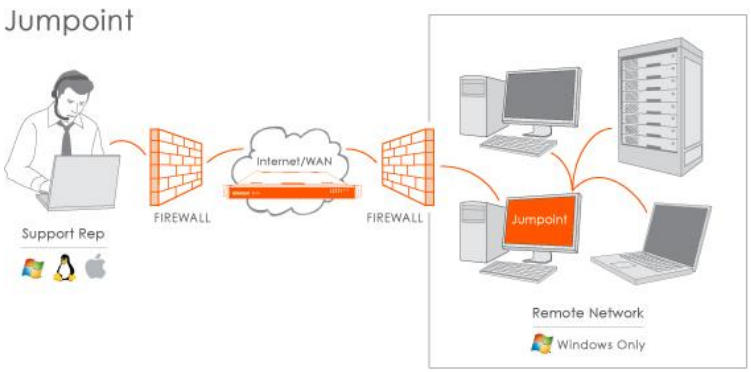
1. Bomgar
2. Dameware
3. mRemote

In de komende paragrafen zijn de drie scenario's beschreven.

7.1 Scenario 1: Bomgar

Bomgar is een applicatie die vrijwel aan alle eisen van igilde voldoet alleen zijn de kosten van de applicatie vrij hoog. Daar moet wel bij gezegd worden dat alle kosten van Bomgar eenmalig zijn. De hardware, de licenties en het onderhoud hoeven slechts eenmalig aangeschaft te worden.

Een voordeel van Bomgar is, is dat het niet noodzakelijk is om een beveiligde VPN verbinding op te zetten of om een eerder besproken opstaphost te gebruiken. Een voordeel hiervan kan zijn dat als het netwerk van de klant dezelfde IP reeks heeft als igilde dat deze niet gewijzigd hoeft te worden om een VPN verbinding mogelijk te maken. Een voordeel van een VPN verbinding is echter dat er een extra beveiligingslaag toegevoegd wordt.



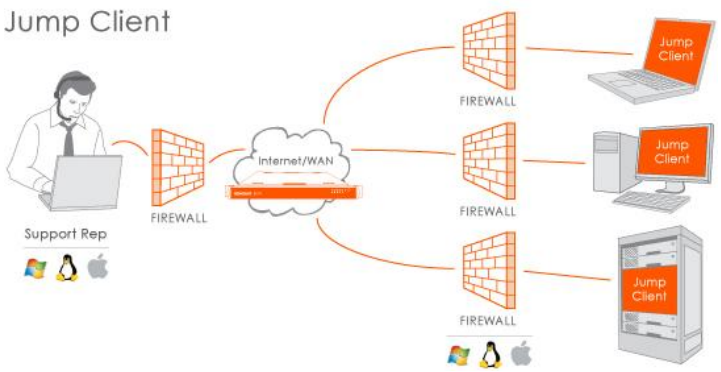
Figuur 5: Werking van Bomgar Jumpoint

Doormiddel van de functie "jumpoint" kunnen externe netwerken eenvoudig toegankelijk gemaakt worden.

Door bijvoorbeeld van een server in het netwerk van een klant een zogenaamd jumpoint te maken kan het netwerk via deze server beheerd worden. Het verkeer loop via de jumpoint server , het is niet nodig om apart op de jumpoint in te loggen om daarna met de andere computers in het netwerk. Er kan rechtstreeks op de externe computer ingelogd worden terwijl het verkeer via de jumpoint server loopt.

Het aanmaken van het installatiebestand voor de jumpoint is eenvoudig via de Bomgar console(of web interface) te realiseren. Dit installatiebestand moet vervolgens handmatig op de betreffende computer geïnstalleerd worden. Doordat Bomgar gebruik maakt van TCP port 80 is het in de meeste gevallen niet nodig om firewalls te configureren. Nadat de jumpoint geïnstalleerd is zoekt deze verbinding met de Bomgar box en is deze beschikbaar in de beheerconsole.

Naast jumpoint kan ook jumpclient gebruikt worden waarmee specifieke systemen ongeacht van hun locatie aangemeld kunnen worden op de Bomgar box. Hiervoor kan een installatiebestand aangemaakt worden voor eenmalige aanmelding van een cliënt of voor een bulk installatie die via een group policy van Microsoft Active Directory verspreidt kan worden. Na de installatie van de jumpclient verschijnt de computer in de beheerconsole.



Figuur 6: Werking van Bomgar Jump Client

Dit zijn de twee manieren waarop de “jump” technologie gebruikt kan worden. Over het LAN netwerk kan de software ook gepusht worden en dan wordt de software automatisch tijdelijk geïnstalleerd. Dit kan alleen als de beheerder in het bezit is van gemachtigde inloggegevens. Na de sessie wordt de software ook weer automatisch gede-installeerd. Dit is bijvoorbeeld mogelijk als er een VPN verbinding met de klant is.

Aan de hand van de bovenstaande informatie zijn er drie procedures mogelijk waarbij er gedacht moet worden aan de volgende punten:

- Beheren van een klantnetwerk met VPN
- AD HOC beheren van een individuele computer
- Beheren van een klantnetwerk zonder VPN

De procedures voor het implementeren van de Bomgar box kan in een aantal eenvoudige stappen uitgelegd worden met de bijbehorende documentatie van Bomgar. Deze documentatie is alleen nog beschikbaar in het Engels en bereikbaar via de support pagina van Bomgar.com.

http://www.bomgar.com/remotedesktopaccess/documents.htm

Actie	Bijbehorend document
1. Plaatsen van de Bomgar box en de eerste configuratie	• B200 Getting started guide
2. Bomgar Basis configuratie	• B200 Appliance Guide
3. Bomgar SSL configuratie	
4. Bomgar Active Directory integratie	• Integrating LDAP For Users Authentication • Integrating RADIUS For Multi-Factor Authentication
5. Gebruik de Bomgar beheer console	• Enterprise Representative User's Guide 10.4 • Standard Administrative User's Guide 10.4

Tabel 6: Procedure voor het in gebruik nemen van de Bomgar Box

7.1.1 Beheren van een klantnetwerk met VPN verbinding

Als de Bomgar box geïnstalleerd is en de beheerders voorzien zijn van de beheerconsole en inloggegevens kan deze gebruikt worden om te starten met remote beheer. In eerste instantie een procedure voor het beheren van de huidige klanten.

Het is vrij eenvoudig om de klanten die al zijn aangesloten via een VPN verbinding te beheren met Bomgar. Deze klanten hebben een privé IP reeks toegewezen gekregen die bij igilde uniek is. Hierdoor is het onmogelijk om overlappingen te krijgen. Hierdoor kunnen klanten uit elkaar gehouden worden doormiddel van de netwerk adressen. Door deze VPN verbindingen is er LAN verkeer mogelijk tussen igilde en de klant.

In Bomgar zit een mogelijkheid om via een LAN de jump technologie te gebruiken. Via de beheerconsole kan simpelweg het IP adres of DNS naam van de te beheren computer ingevuld worden. Als het beheerderwachtwoord wordt ingevuld, wordt er een programma gestart op de cliënt waarna het remote beheer kan beginnen. De procedure die hiervoor geldt staat beschreven in tabel 7:

Actie	Bijbehorend document
1. Log in op de Bomgar beheer console	• Enterprise Representative User's Guide 10.4
2. Klik op de knop start en vul het IP adres of de hostname van de computer in die beheerd moet worden	
3. Vul een beheerwachtwoord in zodra hier om gevraagd wordt en het remote beheer wordt gestart	
4. Overige te beheren objecten kunnen rechtstreeks via de webinterface, putty enz. benaderd worden	

Tabel 7: Beheren van een klantnetwerk met VPN verbinding

Door de firewall van igilde te zo te configureren dat verkeer van igilde naar de klant wordt toegestaan en dat antwoorden hierop ook geaccepteerd worden voorkomt dat klanten een sessie op kunnen zetten richting het netwerk van igilde.

7.1.2 AD HOC beheren van een individuele computer

Bomgar heeft de mogelijkheid om op de computers van klanten die zich op een locatie bevinden die geen verbinding heeft met igilde toch beheer uit te voeren. Deze klanten kunnen naar de website van de Bomgar box gaan, zoals deze is ingesteld bij het plaatsen van de box, om een unieke tijdelijke sessiecode in te vullen die ze van de beheerder krijgen maar er kan ook een e-mail verstuurd worden naar de klant met daarin een directe link voor het starten van het beheer. De procedure hiervoor is beschreven in tabel 8:

Actie	Bijbehorend document
1. Log in op de Bomgar beheer console	• Enterprise Representative User's Guide 10.4
2. Klik op de knop start en genereer een sessiecode	
3. Laat de klant naar de website van de Bomgar box surfen en de code invullen of stuur een e-mail met de link	
4. Laat de klant het tijdelijke bestand downloaden en uitvoeren	
5. Accepteer de binnenkomende sessie in de beheerconsole en voer het beheer uit	

Tabel 8: AD HOC beheren van een individuele computer

Deze technologie ondersteunt alleen grafische besturingssystemen zoals Windows, Ubuntu Desktop, Centos Desktop etc. Na het inloggen op een te beheren computer via deze methode kan het overige netwerk benaderd worden via de benodigde tools, die dan wel aanwezig moeten zijn. Maar dat zal in de meeste gevallen niet nodig zijn omdat deze methode het meest toegepast zal worden bij klanten die op het moment van de aanvraag van beheer zich in een netwerk bevinden wat niet door igilde wordt beheerd.

7.1.3 Beheren van een klantnetwerk zonder VPN

igilde heeft haar huidige klanten zo ingericht dat ze een voor igilde unieke private IP reeks hebben. Hierdoor voorkom je IP adres conflicten bij het opzetten van de VPN verbindingen. Als nieuwe klanten zich aanmelden kan het niet zo zijn dat de klant andere privé adressen moet gaan gebruiken zodat igilde beheer uit kan voeren. Dit moet dus anders opgelost worden.

Door het plaatsen van een eerder genoemde opstaphost in het netwerk van de klant en deze toegankelijk te maken voor igilde creëert een situatie waarbij er via deze opstaphost op het netwerk van de klant ondersteuning geboden kan worden. Bomgar lost dit op door de jump technologie.

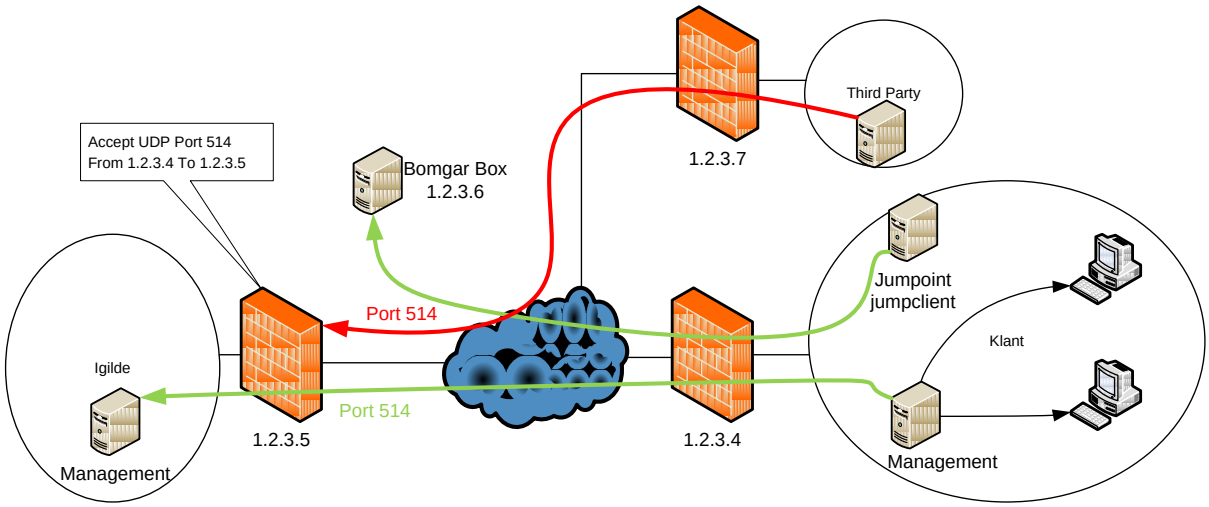
Met de jump technologie kan het netwerk van de klant op twee manieren ingesteld worden. Er kan een netwerk installatie uitgevoerd worden van de jumpclient (figuur 6) die op alle computers de jumpclient installeert. Elke computer maakt dan apart verbinding met de Bomgar box. Als voor deze computers dan een groep aangemaakt wordt in de Bomgar console zijn de computers gemakkelijk over te nemen. Als er één computer of server gebruikt wordt voor het beheer aan het netwerk, worden daar de beheer tools geïnstalleerd, in dit geval putty en de browser kan gebruikt worden voor het beheer aan web interfaces. Het voordeel van de jumptechnologie is dat er geen NAT instellingen nodig zijn omdat de jumpclient een verbinding naar de Bomgar box opzet. Dit gaat via TCP port 80 die over het algemeen in de meeste firewalls al wordt toegestaan.

Een tweede makkelijke manier is om van één of meerdere Windows machines een jumpoint(figuur 5) te maken. Dit gaat doormiddel van het installeren van de software. Deze jumpoints maken net als de jumpclient een verbinding naar de Bomgar box toe. De jumpoints inventariseren de beschikbare computers in het netwerk en stellen deze beschikbaar in de console. In de console kan de jumpoint geselecteerd worden waarna gekozen kan worden welke computer overgenomen moet worden. Na het invullen van een beheerderwachtwoord kan de computer via de jumpoint beheerd worden.

Het is zo dat het niet mogelijk is om via deze jumpoints en jumpcliënts de systemen te monitoren zoals igilde dat doet met Cacti en Nagios®. Dit draait op Linux systemen die de jump technologie niet ondersteunen, dat kan daarom niet gecombineerd worden.

Elke klant aansluiten met een VPN verbinding is niet altijd een optie omdat het kan gebeuren dat klanten dezelfde private IP adressen gebruiken en dat levert conflicten op. Het inrichten van een management systeem in het netwerk van de klant die de interne systemen monitort lost dit probleem op. Dit systeem stuurt deze informatie dan naar het management systeem in het netwerk van igilde die via NAT (Network Address Translation) bereikbaar moet zijn vanaf het internet.

In dit geval mogen alleen de klanten van igilde toegang hebben tot dat systeem. Dit kan door een eenvoudige firewall instelling gerealiseerd worden. Aan de hand van waar de firewall zich bevindt mag alleen het publieke IP adres van de klant toegang hebben op de specifieke TCP/UDP poorten. Over deze poort worden bijvoorbeeld syslog berichten verstuurd vanaf het management systeem van de klant naar het management systeem van igilde. Zie figuur 7.



Figuur 7: Netwerkopstelling eventuele nieuwe situatie

Het management systeem bij de klant verzamelt gegevens van het klantnetwerk. Dit management systeem stuurt deze gegevens door naar het management systeem van igilde. De firewall van igilde staat alleen verbindingen van de klant toe op de specifieke poort hiervoor. Andere partijen kunnen geen toegang krijgen tot deze port, te zien aan de rode lijn die geblokkeerd wordt door de firewall. Een computer in het netwerk van de klant met jumpoint of jumpclient geïnstalleerd kan via port 80 verbinding maken met de Bomgar Box.

Dit principe kan ook andersom werken, waarbij een management systeem van igilde gegevens ophaalt vanaf een systeem bij de klant in plaats van dat het management systeem van de klant de gegevens verstuurd.

Screenshots van Bomgar zijn terug te zien in bijlage 6.

Procedure voor remote beheer met jumpoint

Om een netwerk bereikbaar te maken via een jumpoint moet de procedure zoals beschreven in tabel 9 aangehouden worden.

Actie	Bijbehorend document
1. Bepaal welke Windows computers of servers als jumpoint aangewezen worden. Dit moet een computer zijn die zich in het segment bevindt waarin de computers van de klant zicht bevinden. Aangeraden is om hiervoor een dedicated systeem te gebruiken	• Bomgar Jump Technology User's Guide • Enterprise Representative User's Guide 10.4
2. Maak een nieuw jumpoint aan in de web interface van Bomgar en download het gegenereerde installatiebestand	
3. Installeer jumpoint op de aangewezen computer of server	
4. Maak een jumpclient installatiebestand aan via de web interface van Bomgar	
5. Installeer jumpclient op de aangewezen computer of server (Zodat deze computer ook gebruikt kan worden voor beheer van andere apparatuur)	
6. Installeer zo nodig: Putty of Putty connection manager	
7. Gebruik jumpoint of jumpclient om verbinding te maken met de computer(s) in het externe netwerk	

Tabel 9: Procedure voor remote beheer met jumpoint

Procedure voor remote beheer met jumpclient

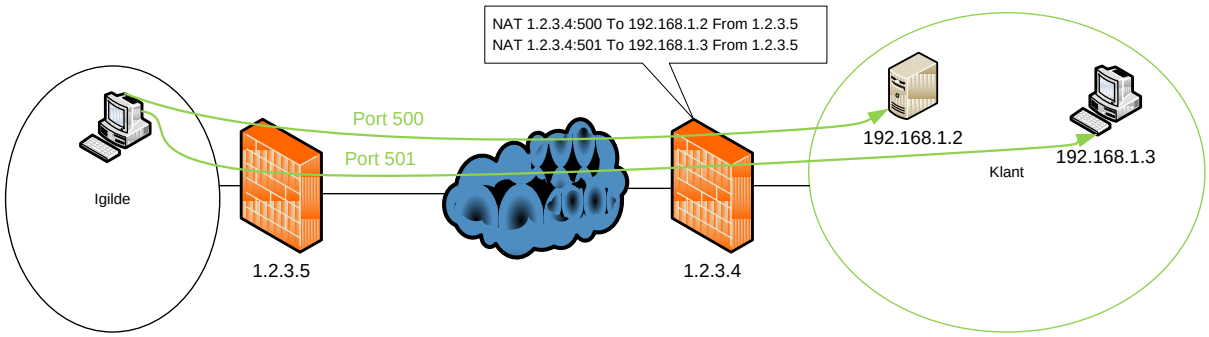
In tabel 10 is beschreven welke procedure aangehouden moet worden als jumpclient gebruikt wordt.

Actie	Bijbehorend document
1. Genereer een jumpclient installatie bestand met de extensie: MSI. En download dit bestand.	• Bomgar Jump Technology User's Guide • Enterprise Representative User's Guide 10.4
2. Plaats dit bestand op een gedeelde map op het netwerk en stel "alleen lezen" rechten in. Of installeer het bestand op een individuele computer en sla stap 3 over.	
3. Laat op elke te beheren computer het volgende script uitvoeren: `msiexec /i pad_naar_bestand.msi KEY_INFO=gegenereerde key`	
4. Gebruik jumpclient om verbinding te maken met de te beheren computer	

Tabel 10: Procedure voor remote beheer met jumpclient

7.2 Scenario 2: DameWare

Als alternatief voor scenario 1 is DameWare naar voren gekomen. Een uitgebreidere uitleg van dit programma is terug te vinden in de paragrafen 6.2.1 en 6.2.2. DameWare vereist IP verkeer over TCP port 6129. DameWare maakt een directe TCP verbinding met de externe computer. Als de computer zich achter een firewall of router bevindt is dit in de meeste gevallen niet mogelijk en moet dit opgelost worden door het openzetten van poorten in de NAT configuratie. Als er zich achter de router of firewall meerdere computers bevinden moet voor elke computer een aparte NAT regel aangemaakt worden met een ander TCP port nummer(figuur 8). Dit is erg omslachtig en vereist een administratie die bijhoud welke port aan welke computer is gekoppeld.



Figuur 8: NAT configuratie als meerdere computers vanaf 1 publiek IP adres bereikt moeten worden

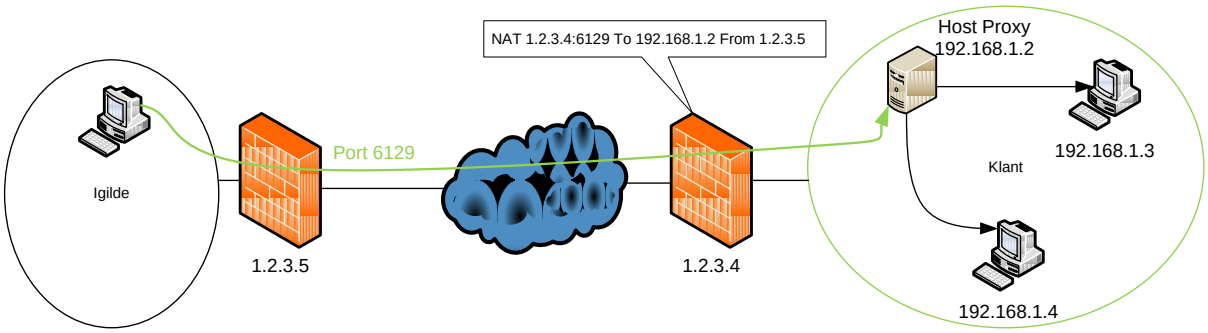
DameWare moet daarom anders gebruikt worden. De klanten die een VPN verbinding hebben met igilde vereisen geen extra instellingen, behalve het installeren van de cliënt software. Zodra het beheerprogramma Dameware NT Utilties op de beheer computer is geïnstalleerd kan dat via de MSI Builder. Hiermee kan een installatiebestand gegenereerd worden met de juiste instellingen. De minimale te wijzigen instellingen moeten zijn:

Instelling	Waarom
Notify on Connect/Disconnect	De gebruiker krijgt een melding zodra er verbinding gemaakt is met de cliënt en als de beheerder de verbinding verbreekt. De klant kan goed zien wat er gebeurd.
Allow only administrators to connect	Alleen gebruikers die lid zijn van de Domain Admin groep van Windows Active Directory mogen verbinding maken met de remote computer.
Permission Required	De klant krijgt een melding waarbij geklikt kan worden of het remote beheer gewenst is of niet.
IP Filter: only accept connections from (IP van management PC)	Een extra beveiligingsoptie waarbij het beheer alleen vanaf specifieke locaties uitgevoerd mag worden.

Tabel 11: Minimale instellingen voor DameWare

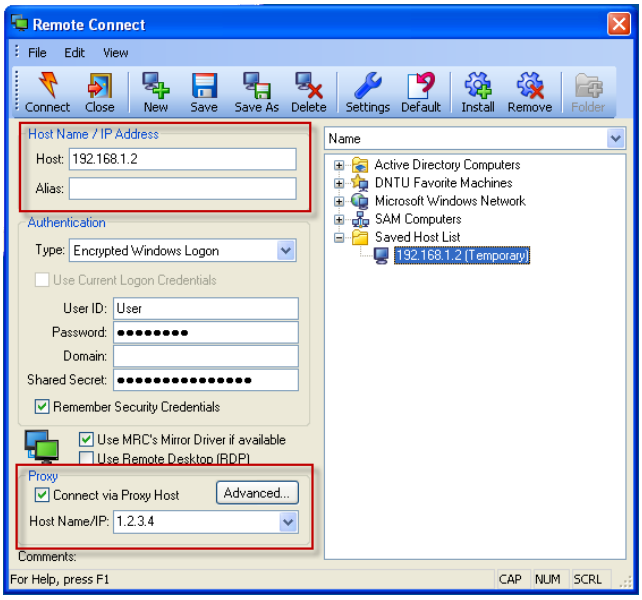
Het verspreiden van dit MSI bestand kan via Active Directory Group Policy gedaan worden.

Vervolgens moeten één of meerdere Windows computers ingesteld worden als “host proxy”. Dit is slechts één instelling. De proxy moet vervolgens bereikbaar gemaakt worden vanaf het internet doormiddel van NAT translatie. De TCP port 6129 moet doorgestuurd worden naar de server die “host proxy” is.



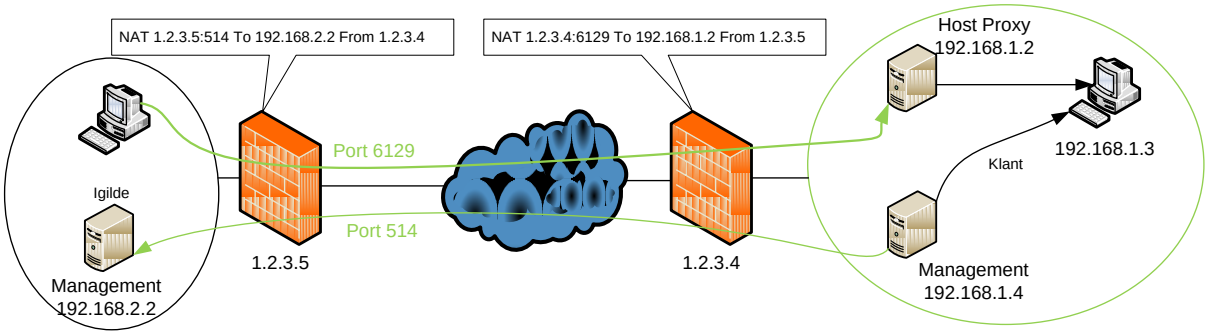
Figuur 9: NAT configuratie voor DameWare Host Proxy

De proxy kan vervolgens gebruikt worden om de andere computers in het netwerk van de klant te bereiken. Het enige wat dan nog gedaan moet worden is de proxy instellen zodra er een computer overgenomen moet worden.



Figuur 10: Screenshot van Proxy instellingen

In figuur 10 is te zien hoe DameWare ingesteld moet worden als vanaf igilde de computer met IP adres 192.168.1.3 overgenomen moet worden. Als “Host” wordt de computernaam of het interne IP adres van de te beheren computer opgegeven en als “Proxy Host” wordt het publieke IP adres van de klant opgegeven die TCP port 6129 forward naar het interne IP adres van de Proxy Host. Uiteraard moet dit in combinatie met een gemachtigde gebruikersnaam en wachtwoord. Het monitoren kan ingesteld worden met eenzelfde principe als bij Bomgar (figuur 7).



Figuur 11: NAT configuratie voor de Host Proxy en het management systeem

Uiteraard moet DameWare geïnstalleerd worden op de computers van de beheerders. Daarna is de procedure voor het configureren voor het gebruik van DameWare beschreven in tabel 12 opgenomen:

Actie	Bijbehorend document
1. Gebruik de DameWare MSI Builder om een netwerk installatie te maken. Dit bestand kan ook gebruikt worden voor individuele installaties. Houd hierbij rekening met eventuele verschillende besturingssystemen. De instellingen die minimaal ingesteld moeten worden staan in tabel 11.	• http://www.dameware.com/support/kb/article.aspx?ID=300090
2. Distribueer dit bestand over het netwerk van de klant. Dit kan doormiddel van automatische software installatie van Microsoft Active Directory.	• http://support.microsoft.com/kb/816102
3. Stel één of meerdere computers/servers in als “Host Proxy”.	• http://www.dameware.com/support/kb/article.aspx?ID=300040
4. Configureer NAT op de internet router. Voor één server alleen port 6129 doorsturen naar de Host Proxy. Bij meerdere Host Proxies moeten de externe portnummers anders worden. Configureer de firewall op de router of op de Proxy Host dat deze alleen connecties vanaf het externe IP van igilde toestaat op de porten van DameWare.	• Vendor afhankelijk
5. Gebruik DameWare om verbinding te maken met een remote computer volgens figuur 10 waarbij gelet moet worden op het IP adres en port nummer van de Host Proxy.	• Figuur 10
6. Neem de Host Proxy over om beheer aan de rest van het netwerk te kunnen doen.	

Tabel 12: Procedure voor het in gebruik nemen van DameWare

Een aantal screenshots van het programma zijn te vinden in bijlage 7.

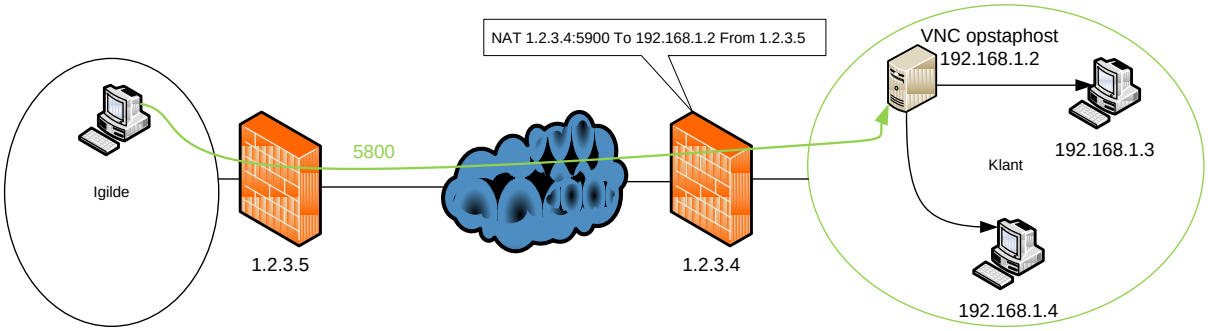
7.3 Scenario 3: mRemote

Als derde en laatste optie is mRemote naar voren gekomen. Een beschrijving van de applicatie is te lezen in paragraaf 6.2.5 en screenshots van het programma staan in bijlage 8.

mRemote heeft meerdere verbindingmogelijkheden waarvan VNC aan de meeste eisen van igilde voldoet. Dit zijn: toestemming vragen aan de klant, klant kan meekijken met beheer en klantwachtwoord hoeft niet gevraagd te worden.

Om gebruik te maken van mRemote moet op elke computer RealVNC server free geïnstalleerd worden. Dit programma is gratis van het internet te downloaden en niet te distribueren. In grote netwerken zal dit enigszins tijdrovend zijn.

Als de RealVNC server op alle computers in het netwerk van de klant geïnstalleerd is en het wachtwoord ingesteld is moeten één of meerdere computers of servers als “opstaphost” ingesteld worden. Hier hoeven verder geen extra instellingen voor gedaan te worden. Er hoeft slechts een NAT regel toegevoegd te worden die de tcp port (5900) van RealVNC doorstuurt naar de “opstaphost” .



Figuur 12: NAT configuratie voor RealVNC

RealVNC viewer, die nodig is om het remote beheer uit te voeren moet zowel op de beheer computer als op de “opstaphost” geïnstalleerd worden. Want zodra het scherm van de “opstaphost” overgenomen is, na het invullen van het correcte wachtwoord, moet opnieuw RealVNC viewer opgestart worden om vervolgens verbinding te maken met de computers in het netwerk van de klant. Net zoals het beheren van de andere elementen wat ook vanaf de opstaphost moet gebeuren.

Om het netwerk van de klant te monitoren wordt hetzelfde principe gebruikt als bij Bomgar (figuur 7).

8 Extra aanbevelingen

In dit document is veel gesproken over een beheerder, beheeraccount of beheerwachtwoord. Een Windows domein heeft een standaard beheeraccount, meestal Administrator. Het is aangeraden om dit account niet te gebruiken voor het uitvoeren van het beheer. Om te voorkomen dat het wachtwoord van dit account achterhaald wordt is het verstandig om een extra account aan te maken om het beheer mee uit te voeren. Het wachtwoord van dit account kan makkelijker aangepast worden omdat het verder nergens voor gebruikt wordt.

Dit zelfde principe geldt voor Linux systemen. Naast de gebruiker “Root” is het verstandig om een extra account toe te voegen voor beheer.

Als voor de “opstaphost” een Windows systeem gebruikt wordt kan in Active Directory ingesteld worden dat alleen specifieke gebruikers in kunnen loggen op dat systeem. Om te voorkomen dat het systeem gebruikt wordt door onbevoegden is dit een goede optie.

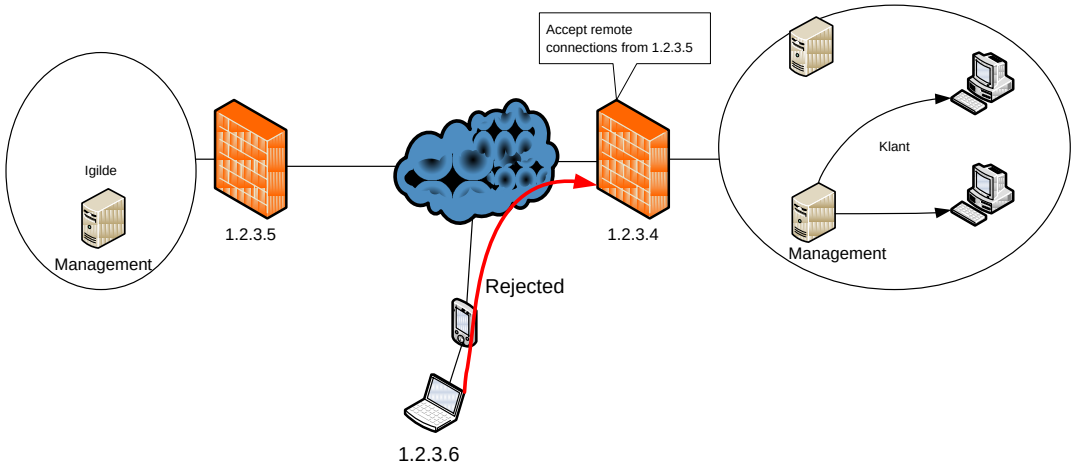
Zoals eerder genoemd is het verstandig om de firewall van igilde zo in te richten dat verkeer naar de klanten met een VPN verbinding worden toegestaan en andersom niet. Door een regel in te stellen dat alleen verkeer naar de klanten wordt toegestaan en de antwoorden hierop wordt voorkomen dat klanten een “nieuwe” sessie op kunnen zetten naar een resource op het netwerk van igilde.

Om te voorkomen dat elke werknemer van igilde naar het netwerk van de klant kan, kan op verschillende manieren opgelost worden. Door het inrichten van een specifiek VLAN wat alleen toegang heeft tot de klanten en hier de computers in te zetten die toegang moeten hebben tot klantnetwerken voorkomt dat iedereen toegang heeft. Een extra uitbreiding hierop is dat er mogelijkheden zijn om aan de hand van de ingelogde gebruiker te bepalen in welk VLAN de computer moet komen. Aan deze optie is wegens tijdsgebrek geen aandacht besteed.

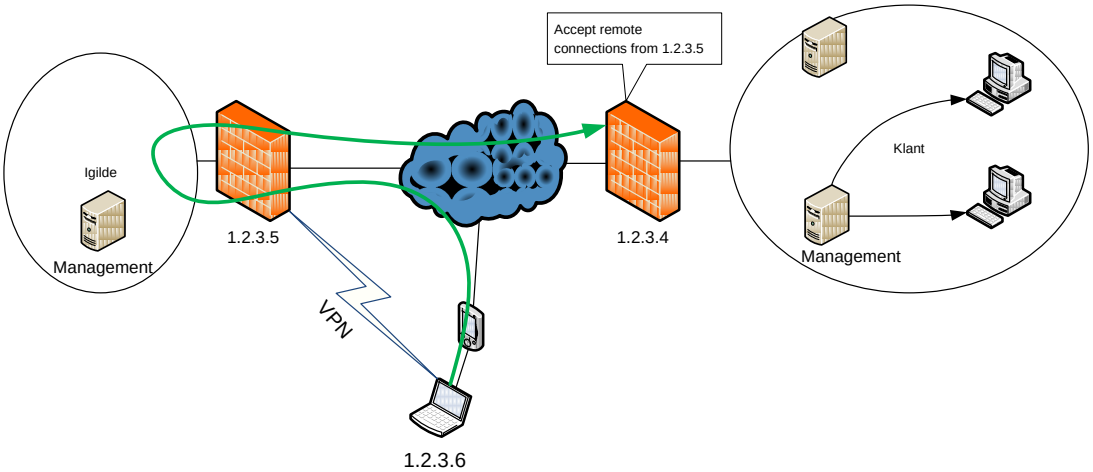
9 Mobiele werker

igilde wenst graag beheer uit te kunnen voeren vanaf mobiele locaties. Bijvoorbeeld onderweg of op andere plekken waar geen internet verbinding beschikbaar is. De werknemers van igilde hebben allemaal een telefoon van de zaak met een onbeperkte data verbinding die toegang geeft tot het internet. Naast hun telefoon hebben ze ook altijd een laptop bij zich. Door de telefoon aan te sluiten aan de laptop kan de internet verbinding doorgezet worden naar de laptop.

Nu de laptop verbinding heeft met het internet kan er nog geen verbinding gemaakt worden met de klanten omdat de firewall instellingen dit blokkeren. Alleen het igilde netwerk heeft hier toegang toe. Dit is te omzeilen door een functie die igilde al gebruik. De werknemers kunnen met een Cisco VPN cliënt toegang krijgen tot het bedrijfsnetwerk. Logischer wijs kan er na het opzetten van de VPN verbinding via het netwerk van igilde beheer uitgevoerd worden.



Figuur 13: Rechtstreeks remote beheer vanaf een mobiele locatie is niet toegestaan



Figuur 14: Remote beheer vanaf een mobiele locatie kan wel door het opzetten van een VPN verbinding naar het bedrijfsnetwerk van igilde.

10 Conclusie

Gezien de drie scenario's die als advies worden aangeboden aan igilde kunnen de volgende conclusies getrokken worden:

- Bomgar is prijzig maar is qua functies en extra veiligheidsopties de beste ten opzichte van DameWare en mRemote.
- Voor Bomgar zijn nauwelijks extra instellingen nodig, de implementatie is eenvoudig.
- Bomgar draait op standaard poort 80 wat de implementatie wederom vereenvoudigd.
- Bomgar heeft een functie SSH Jump geïntegreerd in een nieuwe software versie die medio December is uitgekomen waar geen aandacht aan besteed is.
- Bomgar heeft een eindejaar aanbieding gedaan waarvan de kosten ruim $3000 lager liggen.
- Er bestaat een goedkoper alternatief voor Bomgar waarbij een B100 Bomgar Box aangeschaft wordt, upgraden kan altijd.
- DameWare is geen minderwaardig alternatief voor Bomgar.
- DameWare vereist wat meer configuratietijd omdat hier onder andere firewalls goed ingesteld moeten worden omdat DameWare op een vreemde poort draait.
- Als goedkopere oplossing zal DameWare Mini Remote Control voldoende zijn in plaats van de extra Functie die NT Utilities biedt.
- De beveiliging van mRemote is minimaal, deze optie wordt daarom ook niet aangeraden
- Het implementeren van RealVNC om mRemote te gebruiken met de gewenste eisen van igilde is tijdrovend omdat elke computer handmatig geïnstalleerd moet worden.
- mRemote heeft het beheren van SSH servers en web interfaces goed geïntegreerd maar dit weegt niet op tegen de nadelen.
- Als mRemote een betere beveiliging had, was de concurrentie veel groter geweest.

Aangezien Bomgar een prijzige oplossing is zal de voorkeur eerder uitgaan naar DameWare. mRemote heeft te veel nadelen ten opzichte van de andere twee oplossingen en zal dus zeer waarschijnlijk afvallen bij de uiteindelijke keuze. Technisch gezien is er echter wel met alle drie de applicaties een werkbare situatie te creëren.

Evaluatie

Het project is nagenoeg goed verlopen. Het onderzoek is een heel stuk uitgelopen waardoor ik aan het eind toch een beetje in de knel ben gekomen en niet heel veel ruimte gehad heb om terugkoppeling te krijgen vanuit de Hogeschool Utrecht. Door de drukke bezetting van mijn begeleider kon dit ook niet op korte termijn. Wat erg lastig was.

Qua inhoud van het project heb ik niet alle punten goed kunnen behandelen. Onder andere het onderwerp out band management ben ik helemaal niet aan toegekomen, wat ik zelf wel jammer vind. Had me hier graag ook wat verder in verdiept omdat ik het een interessant onderwerp vindt.

Het was spannend om een project als dit binnen een hele specifieke tijd alleen uit te moeten voeren in een vreemde omgeving en er achter te komen, hoe goed je ook plant je altijd obstakels tegenkomt. In mijn geval voornamelijk met de tijd. Aan het begin van het project liep alles mooi op schema, maar halverwege ben ik met het onderzoek ver uitgelopen omdat het veel tijd heeft gekost om de verschillende applicaties te testen. Hierdoor heb ik onder andere het schrijven van de scriptie te veel uitgesteld. Terwijl ik hier op tijd mee begonnen ben maar het heeft een tijd stil gelegen door het onderzoek. Een volgende keer moet ik eerder ingrijpen door het onderzoek in te krimpen.

Wel heb ik netjes alle fasen doorlopen. Eerst de ene fase afronden voordat de andere fase begint. Hier heb ik veel van geleerd, omdat het een beter inzicht geeft in de status van het project.

Door het uitstellen heb ik op het laatste moment meer last gehad van de tijdsdruk maar heb binnen de tijd met een aantal overuren naar mijn mening toch een mooi resultaat neergezet. Jammer dat door de tijdsdruk de terugkoppeling naar de Hogeschool Utrecht niet foutloos liep.

Ik heb een bijeenkomst gehad met de begeleider van de Hogeschool Utrecht waarbij ik niet goed begrijpelijk overkwam. Hierdoor ben ik heel erg gaan twijfelen of ik het inderdaad fout gedaan had. Nadat ik het een en ander nagevraagd had bij igilde bleek dit gelukkig mee te vallen.

Ik vond het heel leuk om dit project uit te voeren bij igilde. Ik ben zo veel mogelijk op de werkvloer geweest om ook de werksfeer, die altijd heel gezellig is van igilde te proeven, en heb hier en daar ook werkzaamheden uit kunnen voeren. Ik vond het prettig werken met de werknemers van igilde.

Iedere week, tijdens het werkoverleg van igilde heb ik mijn zegje gedaan om iedereen op de hoogte te houden van de status van het project. Dit is aan de hand van een opmerking van de Hogeschool Utrecht in een vroeg stadium ingevoerd.

Ik vond het leuk om dit project uitgevoerd te hebben en hoop het met een positief resultaat af te sluiten.

Woordenlijst

Remote beheer

Het op afstand hulp bieden en onderhoud plegen aan de netwerken van klanten

Beheerder

De persoon die zich achter de beheer computer bevindt en ondersteuning biedt aan het te beheren object.

IP Adres

Een IP-adres is een getal dat een host op het Internet of op een intranet identificeert.

VPN (Virtual Private Network)

Ontworpen om via openbare netwerken (lees internet) toch een veilige verbinding te kunnen realiseren. Hiertoe maakt VPN gebruik van het Point-to-Point Tunneling Protocol (PPTP) en creëert het een aparte Dial-Up Adapter, zodat via Dial-Up Networking ingelogd kan worden.

Telnet

Het protocol Telecommunications Network (kortweg Telnet) wordt gebruikt als netwerkprotocol op het Internet en lokale netwerken. Het in 1969 ontwikkeld protocol (RFC 15, gestandaardiseerd als IETF STD8) was een van de eerste echte internetstandaarden. Behalve de naam van het protocol staat de naam ook voor de cliënt, welke de server kan benaderen voor het op afstand configureren ervan. Aangezien het protocol qua beveiliging niet goed genoeg is, is dit protocol op veel platforms vervangen door SSH.

SSH (Secure Shell)

Een geactualiseerde, veiliger versie van Telnet.

DNS (Domain Name Service)

DNS biedt naamomzettingsservices voor cliënt toepassingen. DNS is een gedistribueerde database die host- en domeinnamen en de daarbij behorende IP-adressen bevat. Door DNS is het niet langer nodig om op elke computer een lijst met IP-adressen te onderhouden. DNS zorgt er namelijk voor dat de lijst beschikbaar is op een aantal verschillende computers in het netwerk.

GPRS (General Packet Radio Service)

De snelle verbinding voor WAP-telefoons. Met deze techniek is mobiel internetten en e-mail mogelijk zonder steeds opnieuw in te moeten bellen; je bent altijd online en betaalt voor de data die je verzendt. Omdat via GPRS ook kan worden ingelogd op een intranet (bedrijfsnetwerk) is de veiligheid uitvoerig getest. In feite is de werking van GPRS te vergelijken met die van een LAN: gegevens worden in de vorm van digitale pakketten verzonden.

NAT (Network Address Translation)

Methode die specifiek bedoeld is om meerdere gebruikers dezelfde internettoegang te laten gebruiken. Hierbij wordt gebruik gemaakt van de mogelijkheid van het IP-protocol om het IP-adres te veranderen in een ander IP-adres. Hierdoor kan het interne IP-adres van het werkstation dat het internet op wil worden vervangen door een extern adres.

TCP (Transmission Control Protocol)

TCP is verantwoordelijk voor de betrouwbare verzending van gegevens van het ene knooppunt op het netwerk naar het andere. TCP brengt een verbindingsgeoriënteerde sessie, of virtueel circuit, tot stand tussen twee computers. De verbinding met een andere computer wordt gemaakt door een pakket te verzenden waarin de doelhost wordt gevraagd of het mogelijk is een verbinding tot stand te brengen. Vervolgens wacht TCP of de computer beschikbaar is voor communicatie. Als de doelcomputer online is en luistert, reageert deze door een bericht te sturen: 'Ik ben beschikbaar voor communicatie en hoor graag meer van je'. Hierop reageert de eerste computer als volgt: 'Mooi, hier is de rest van de informatie.' Dit proces van het tot stand brengen van een verbinding wordt de 'three-way handshake' genoemd. Met dit proces wordt vastgesteld welk poortnummer er moet worden gebruikt en wat de ISN's van de beide partijen zijn. De computers die een verbinding met elkaar tot stand brengen en onderhouden, moeten bepaalde vitale gegevens met elkaar uitwisselen. Elk TCP-pakket dat wordt verzonden bevat een bron- en doel-TCP-poortnummer, een opvolgingsnummer voor berichten die in kleinere gedeelten moeten worden verzonden en een controlesom om ervoor te zorgen dat de informatie foutloos wordt verzonden. Daarnaast bevat elk pakket een bevestigingsgetal dat de broncomputer vertelt welke onderdelen van het bericht op de bestemming zijn aangekomen. Elk pakket bevat tevens een metrische waarde voor de grote van het TCP venster om flow control tussen beide computers mogelijk te maken.

UDP (User Datagram Protocol)

UDP is een protocol in de transportlaag van het TCP/IP-model dat verantwoordelijk is voor eind-tot-eind gegevensoverdracht op een netwerk. Het maakt gebruik van datagrammen om zijn informatie te ontvangen en versturen. In vergelijking met het Transmission Control Protocol is het User Datagram Protocol veel efficiënter in de gegevensoverdracht, omdat het User Datagram Protocol heel weinig overhead aan de data toevoegt. In tegenstelling tot TCP is UDP een verbindingsloos protocol. Er wordt dan ook geen sessie tot stand gebracht. UDP probeert niet te controleren of de doelhost de verzonden informatie daadwerkelijk ontvangt. UDP wordt gebruikt door toepassingen die kleine hoeveelheden gegevens verzenden die geen afleveringsgarantie vereisen.

Syslog

Een standaard om log gegevens door te sturen over een IP netwerk.

SNMP (Simple Network Management Protocol)

Raamwerk voor het beheren van een netwerk. Simple Network Management Protocol, deze zorgt ervoor dat de netwerkbeheerder supervisie op het netwerk houdt met programma's van verschillende leveranciers. SNMP is een standaard die vrijwel elke leverancier ondersteunt. De onderdelen waaruit SNMP is opgebouwd bestaan uit een management-agent, MIB's, een SNMP-protocol-agent en het netwerktransport-protocol. Een TCP/IP protocol om netwerken te bewaken. Bij SNMP bewaken kleine utilities, agents, het netwerkverkeer en -gedrag in cruciale netwerkonderdelen teneinde statistische gegevens te verzamelen en ze op te slaan in een Management Information Base (MIB). Om de gegevens in een bruikbare vorm te verzamelen pollt een speciaal management-console-programma de agents en brengt informatie over naar hun MIB's. Komt een gegeven boven of onder parameters die de netwerkmanager heeft ingesteld, dan kan het management-console-programma boodschappen op het beeldscherm zetten die aangeven waar zich een probleem voordoet en een waarschuwing sturen naar onderhoudsmedewerkers door automatisch een oproepnummer te kiezen. SNMP-beheer is gebaseerd op agents, die met elkaar communiceren. SNMP gebruikt meestal IP als basis-protocol en komt het meest voor in high-end Lan-Management software.

RDP (Remote Desktop Protocol)

Een protocol van Microsoft voor de terminal server. Met dit protocol communiceert de cliënttoepassing met de terminal server. Er zijn RDP cliënttoepassingen van Microsoft beschikbaar voor de diverse Windows versies.

Group Policy

Group policy's definiëren bepaalde instellingen voor groepen gebruikers en computers om het beheer te vereenvoudigen.

LDAP (Lightweight Directory Access Protocol)

Stel u hebt een bedrijf met duizend werknemers; die hebben allemaal een e-mailadres, doorkiesnummer en uiteraard een voor- en achternaam. Nu moet u voor al die gebruikers mailboxen creëren. Vervolgens installeert u een proxy- en een FTP-server, en daar moeten dezelfde gebruikers nog eens op worden herkend. Gaat u dit allemaal handmatig invoeren? Vroeger moest dit, omdat uitwisseling van gebruikersgegevens onmogelijk was, of te ingewikkeld. Daarom is LDAP ontwikkeld. Dit protocol is ontwikkeld op de X.500-standaard. Dit is een standaard voor directory services (database over gebruikersinformatie). Met LDAP is het mogelijk om op een relatief eenvoudige manier gegevens over gebruikers over het Internet te versturen. Novell gebruikt LDAP bijvoorbeeld om alle instellingen van gebruikers op een logische manier op te slaan. Dit protocol wordt onder ander toegepast om de Active Directory van Windows te lezen, te veranderen en te doorzoeken.

RADIUS (Remote Access Dial-In User Service

Cliënt/server protocol dat via authenticatie de identiteit van een gebruiker vaststelt en toegang geeft tot een systeem of dienst.

RSA (Rivest, Shamir en Adleman)

Asymmetrische versleutelingsalgoritme. De betrouwbaarheid van de sleutel is afhankelijk van de sleutellengte. Sleutels met een lengte van 40-bits werden al met succes aangevallen. Sleutel lengtes met meer dan 128-bits zijn al een stuk betrouwbaarder, voor het breken van een dergelijke code is veel rekencapaciteit nodig.

DSA (Directory System Agent)

Onderdeel van X.500. Het proces dat de fysieke opslag van Active Directory beheert. Zorgt voor de directoryservice voor een sub-net of groep.

AES (Advanced Encryption Standard)

Een standaard om informatie te encrypten (versleutelen). Hierbij wordt gebruik gemaakt van 128-, 192- en 256-bits sleutels.

X.500

De door de ISO (International Standards Organization) als Directory Service binnen het OSI-model (Open Systems Interconnnect ontwikkelde en door de ITU (International Telecommunications Union) overgenomen standaard. De Directory Service maakt het mogelijk om toegang te krijgen tot alle objecten binnen de directory. Deze objecten kunnen informatie bevatten over computers, diensten, bestandsresources, personen, bedrijven, enzovoort. De directory organiseert alle objecten in een hiërarchische structuur, die bijvoorbeeld is gerangschikt volgens landen, organisaties en suborganisaties. X.500 is een zeer omvangrijke definitie voor een Direcotry Service, waardoor de implementaties ervan nogal veel resources vergen. Om deze problemen te omzeilen, werd LDAP voor het gebruik van een Directory Service met 'kleine' cliënts in het leven geroepen.

Kerberos

Een autorisatieprotocol, gedefinieerd door de Internet Engineering Task Force (IETF) in RFC1510, dat een gedistribueerde autorisatie tussen zowel cliënt als server aangeeft. Dit protocol is ontwikkeld bij MIT en is gebaseerd op een variant van Needham-Schroeder. Kerberos wordt onder andere gebruikt in Windows. De beveiliging komt hierop neer: wanneer een cliënt een server wil benaderen - en dus ook vice versa voor het antwoord - moeten beide partijen elkaar kunnen vertrouwen. Om authenticatie mogelijk te maken wordt binnen Kerberos gebruik gemaakt van een derde partij die door de twee andere partijen wordt vertrouwd. Deze derde partij is bij Windows het Kerberos Key Distribution Center (KDC), een service die op elke Windows domain controller draait. Een gebruiker die succesvol inlogt op Windows ontvangt van het KDC een Ticket Granting Ticket (TGT). Hierin zit de session key voor de gebruiker opgesloten. Met gebruik van de session key en het TGT kan nu een tweede session key aangevraagd worden om een bepaalde resource te benaderen. De resource moet erop kunnen vertrouwen dat de gebruiker is wie hij zegt te zijn. Al met al is de manier waarop Kerberos de beveiliging regelt complex, maar wel erg veilig.

Bronvermelding

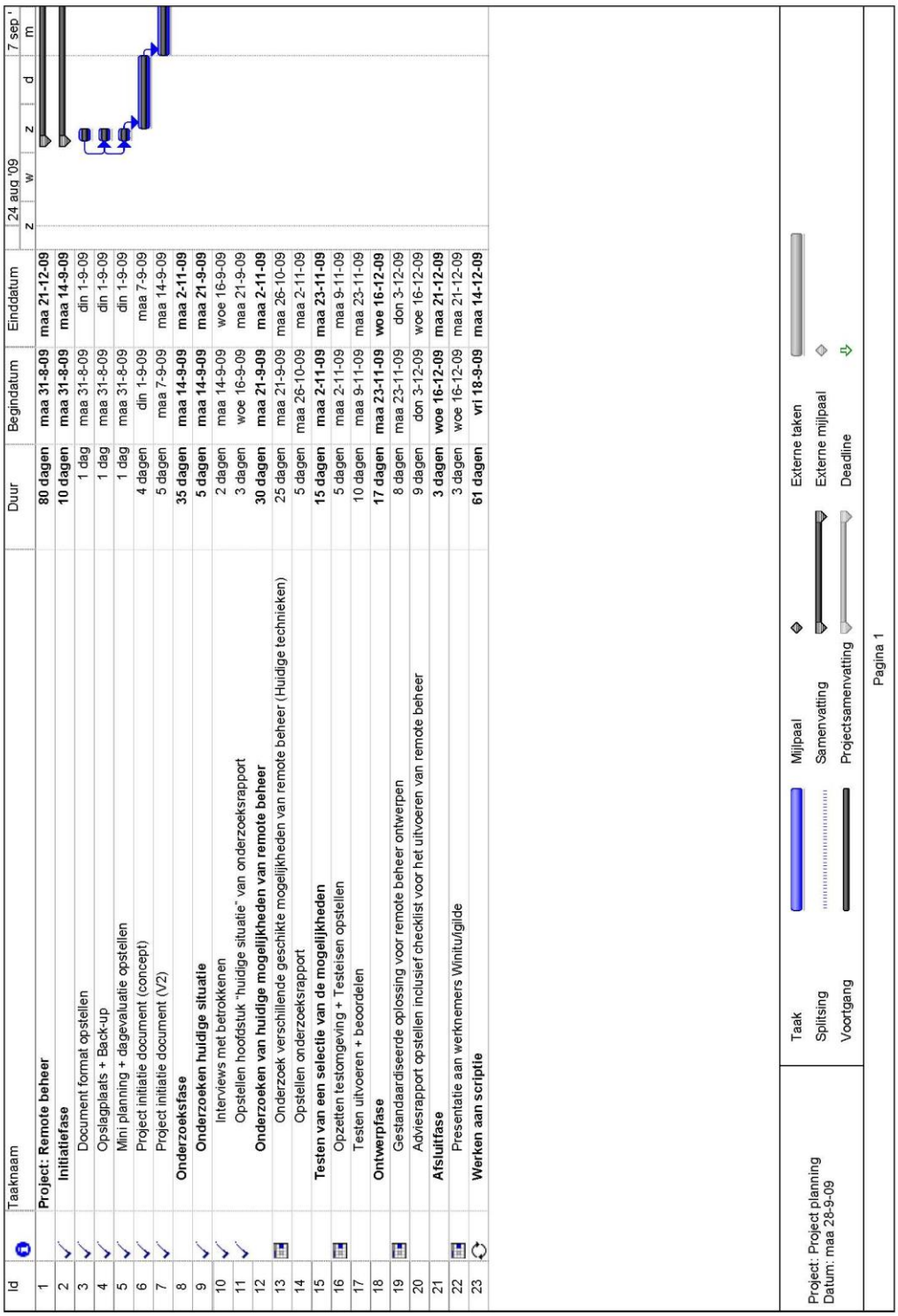
De bronnen die tijdens het project geraadpleegd zijn staan beschreven in tabel 13.

Bron	Omschrijving
http://en.wikipedia.org/wiki/FIPS_140-2	Beknopte omschrijving wat FIPS 140-2 inhoud met de verschillende niveaus.
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	De volledige FIPS 140-2 documentatie.
http://www.tech-faq.com/fcaps.shtml	Beknopte omschrijving van FCAPS.
http://www.dameware.com/products/	Informatie over DameWare producten.
http://www.pjtec.com	Informatie over Goverlan producten.
http://www.radmin.com	Informatie over de applicatie: Radmin.
http://www.mremote.org	Informatie over de applicatie: mRemote.
http://www.simple-help.com	Informatie over de simple-help producten.
http://www.bomgar.com	Informatie over Bomgar.
http://www.vandyke.com	Informatie over de applicaties: secureCRT en secureFX.
http://puttycm.free.fr/cms/	Informatie over de applicatie: putty connection manager.
http://support.microsoft.com/kb/816102	Handleiding als naslagwerk voor het opzetten van de testomgeving.
http://www.computerwoorden.nl	Pagina met uitleg over heel veel woorden in de computer wereld.
http://www.realvnc.com	Website van het programma RealVNC

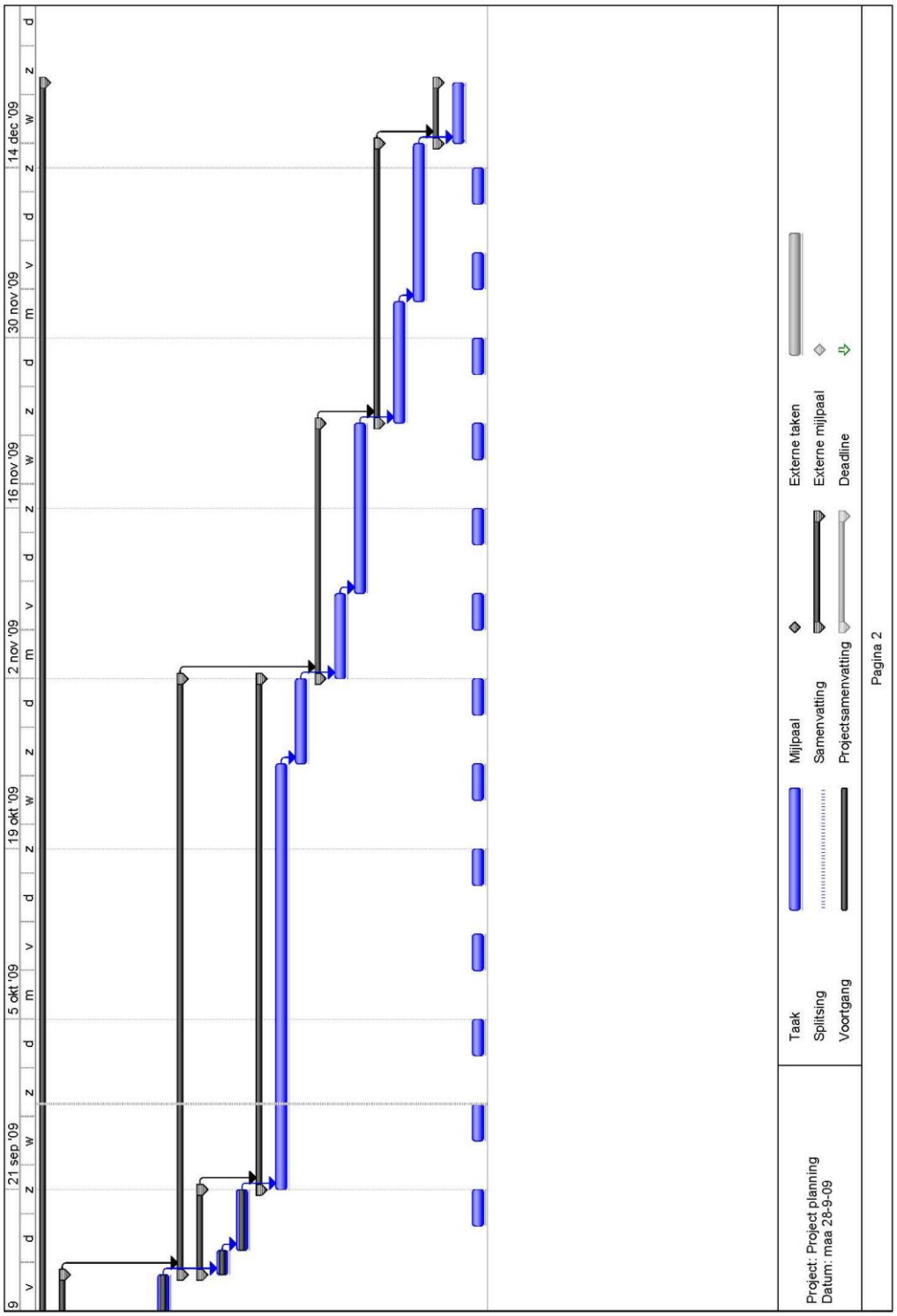
Tabel 13: Bronnen

Bijlagen

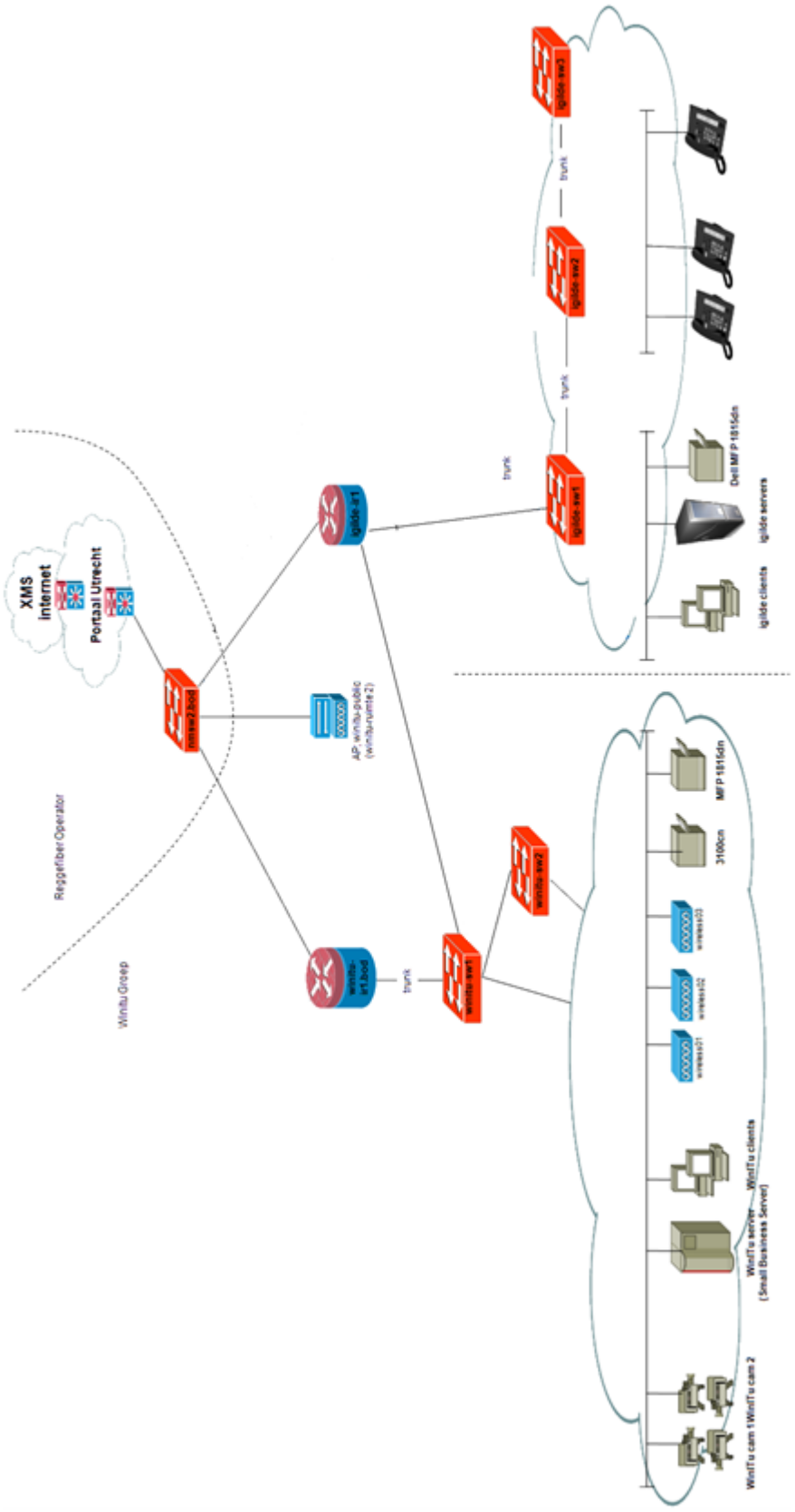
Bijlage 1: Projectplanning



Id	Taaknaam	Duur	Begindatum	Einddatum
1	**Project: Remote beheer**	**80 dagen**	**maa 31-8-09**	**maa 21-12-09**
2	**Initiatiefase**	**10 dagen**	**maa 31-8-09**	**maa 14-9-09**
3	Document format opstellen	1 dag	maa 31-8-09	din 1-9-09
4	Opslagplaats + Back-up	1 dag	maa 31-8-09	din 1-9-09
5	Mini planning + dagevaluatie opstellen	1 dag	maa 31-8-09	din 1-9-09
6	Project initiatie document (concept)	4 dagen	din 1-9-09	maa 7-9-09
7	Project initiatie document (V2)	5 dagen	maa 7-9-09	maa 14-9-09
8	**Onderzoeksfase**	**35 dagen**	**maa 14-9-09**	**maa 2-11-09**
9	**Onderzoeken huidige situatie**	**5 dagen**	**maa 14-9-09**	**maa 21-9-09**
10	Interviews met betrokkenen	2 dagen	maa 14-9-09	woe 16-9-09
11	Opstellen hoofdstuk "huidige situatie" van onderzoeksrapport	3 dagen	woe 16-9-09	maa 21-9-09
12	**Onderzoeken van huidige mogelijkheden van remote beheer**	**30 dagen**	**maa 21-9-09**	**maa 2-11-09**
13	Onderzoek verschillende geschikte mogelijkheden van remote beheer (Huidige technieken)	25 dagen	maa 21-9-09	maa 26-10-09
14	Opstellen onderzoeksrapport	5 dagen	maa 26-10-09	maa 2-11-09
15	**Testen van een selectie van de mogelijkheden**	**15 dagen**	**maa 2-11-09**	**maa 23-11-09**
16	Opzetten testomgeving + Testeisen opstellen	5 dagen	maa 2-11-09	maa 9-11-09
17	Testen uitvoeren + beoordelen	10 dagen	maa 9-11-09	maa 23-11-09
18	**Ontwerpfase**	**17 dagen**	**maa 23-11-09**	**woe 16-12-09**
19	Gestandaardiseerde oplossing voor remote beheer ontwerpen	8 dagen	maa 23-11-09	don 3-12-09
20	Adviesrapport opstellen inclusief checklist voor het uitvoeren van remote beheer	9 dagen	don 3-12-09	woe 16-12-09
21	**Afsluitfase**	**3 dagen**	**woe 16-12-09**	**maa 21-12-09**
22	Presentatie aan werknemers Winitu/igilde	3 dagen	woe 16-12-09	maa 21-12-09
23	**Werken aan scriptie**	**61 dagen**	**vri 18-9-09**	**maa 14-12-09**


21 sep '09
5 okt '09
19 okt '09
2 nov '09
16 nov '09
30 nov '09
14 dec '09
Taak
Splitsing
Voortgang
Mijlpaal
Samenvatting
Projectsamenvatting
Externe taken
Externe mijlpaal
Deadline
Project: Project planning
Datum: maa 28-9-09
Pagina 2

Bijlage 2: Overzicht igilde netwerk



Bijlage 3: Kostenoverzicht

	Licentiemodel	Frequentie	Benodigdheden	Verwachte aantal	Kosten	Subtotaal	Totaal in $	Totaal in €
DameWare Mini Remote	Per gebruiker	Eenmalig	Licentie	5	$90	$450	$450	€ 303
DameWare NT Utilities	Per gebruiker	Eenmalig	Licentie	5	$289	$1.445	$1.445	€ 972
Goverlan Remote Control	Per gebruiker	Eenmalig	Licentie	4	$699	$2.796	$3.592	€ 2.415
		Jaarlijks	Upgrades	4	$199	$796		
Radmin	Per computer	Eenmalig	Helpdesk licentie	150	€ 25	€ 3.750	-	€ 3.750
mRemote	-	-	-	-	-	-	-	€ 0
simplegateway	Per actieve sessie	Eenmalig	Licentie	5	-	$895	$895	€ 602
smartCode VNC manager	Per gebruiker	Jaarlijks	Licentie	5	-	$534,38	$534	€ 359
Bomgar	Per actieve sessie	Eenmalig	Licentie	5	-	$18.149	$18.149	€ 12.202
			Bomgar Box	1	-			
SecureCRT	Per gebruiker	Eenmalig	Licentie	4	$99	$396	396	€ 266
Putty Connection Manager	-	-	-	-	-	-	-	€ 0

Bijlage 4: scoretabel

	Windows	Linux	Web enabled devices	SSH	Telnet	RDP Mogelijk?	X86	X64	Toestemming geven mogelijk?	Server Software?	Client software?	Client software distribueerbaar?	Extra mogelijkheden?	Windows authenticatie	Klantwachtwoord nodig?	Alleen toegankelijk voor beheerders?	Bios configureerbaar?	Freeware	Kosten	compatible met opstaphost?	Extern toetsenbord/muis uitschakkelen?	Bandbreedteverbruik	FIPS Niveau	Totaal
DameWare Mini Remote	4	0	0	0	0	1	2	2	2	2	2	3	2	4	3	2	2	0	0	2	2	2	2	41
DameWare NT Utilities	4	0	0	0	0	1	2	2	2	2	2	3	2	4	3	2	2	0	0	2	2	2	2	41
Goverlan Remote Control	2	1	0	0	0	0	2	2	2	2	2	3	2	2	0	2	2	0	0	2	2	2	1	33
Radmin	3	0	0	0	0	0	2	2	2	2	2	2	0	3	2	2	2	1	0	2	2	2	1	30
mRemote	2	1	2	2	2	2	2	2	2	2	1	2	1	0	1	1	2	0	4	4	2	1	3	39
simplegateway	2	2	0	0	0	0	0	2	2	0	1	2	0	0	0	2	2	0	0	3	1	0	2	21
smartCode VNC manager	2	1	0	0	0	0	2	2	2	2	3	3	3	0	2	2	2	0	0	3	3	2	1	35
Bomgar	**3**	**2**	**0**	**0**	**0**	**0**	**2**	**2**	**2**	**2**	**4**	**3**	**3**	**4**	**2**	**2**	**2**	**0**	**0**	**0**	**4**	**2**	**2**	**42**
SecureCRT	0	2	0	3	2	0	2	2	2	0	2	2	0	3	2	2	2	0	0	3	2	0	4	33
Putty Connection Manager	0	2	0	3	2	0	2	2	2	0	2	2	0	3	2	2	2	0	4	4	2	0	4	38
Remote Desktop	2	0	0	0	0	0	2	2	2	0	2	2	2	2	2	0	2	0	0	0	2	0	1	23

Bijlage 5: FIPS 140-2

1. OVERVIEW

This standard specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

FIPS 140-1 was developed by a government and industry working group composed of both operators and vendors. The working group identified requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and life protecting data) and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Four security levels are specified for each of 11 requirement areas. Each security level offers an increase in security over the preceding level. These four increasing levels of security allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments. FIPS 140-2 incorporates changes in applicable standards and technology since the development of FIPS 140-1 as well as changes that are based on comments received from the vendor, laboratory, and user communities.

While the security requirements specified in this standard are intended to maintain the security provided by a cryptographic module, conformance to this standard is not sufficient to ensure that a particular module is secure. The operator of a cryptographic module is responsible for ensuring that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted.

Similarly, the use of a validated cryptographic module in a computer or telecommunications system is not sufficient to ensure the security of the overall system. The overall security level of a cryptographic module must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilized and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilize cryptographic modules provide an acceptable level of security for the given application and environment.

The importance of security awareness and of making information security a management priority should be communicated to all users. Since information security requirements vary for different applications, organizations should identify their information resources and determine the sensitivity to and the potential impact of losses. Controls should be based on the potential risks and should be selected from available controls, including administrative policies and procedures, physical and environmental controls, information and data controls, software development and acquisition controls, and backup and contingency planning.

The following sections provide an overview of the four security levels. Common examples, given to illustrate how the requirements might be met, are not intended to be restrictive or exhaustive.

1.1 Security Level 1

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

Security Level 1 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system. Such implementations may be appropriate for some low-level security applications when other controls, such as physical security, network security, and administrative procedures are limited or nonexistent. The implementation of cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements.

1.2 Security Level 2

Security Level 2 enhances the physical security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or for pick-resistant locks on removable covers or doors of the module. Tamper-evident coatings or seals are placed on a cryptographic module so that the coating or seal must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorized physical access.

Security Level 2 requires, at a minimum, role-based authentication in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform a corresponding set of services.

Security Level 2 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that

- meets the functional requirements specified in the Common Criteria (CC) Protection Profiles (PPs) listed in Annex B and
- is evaluated at the CC evaluation assurance level EAL2 (or higher).

An equivalent evaluated trusted operating system may be used. A trusted operating system provides a level of trust so that cryptographic modules executing on general purpose computing platforms are comparable to cryptographic modules implemented using dedicated hardware systems.

1.3 Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroizes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

Security Level 3 requires identity-based authentication mechanisms, enhancing the security provided by the role-based authentication mechanisms specified for Security Level 2. A cryptographic module authenticates the identity of an operator and verifies that the identified operator is authorized to assume a specific role and perform a corresponding set of services.

Security Level 3 requires the entry or output of plaintext CSPs (including the entry or output of plaintext CSPs using split knowledge procedures) be performed using ports that are physically separated from other ports, or interfaces that are logically separated using a trusted path from other interfaces. Plaintext CSPs may be entered into or output from the cryptographic module in encrypted form (in which case they may travel through enclosing or intervening systems).

Security Level 3 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that

- meets the functional requirements specified in the PPs listed in Annex B with the additional functional requirement of a Trusted Path (FTP_TRP.1) and
- is evaluated at the CC evaluation assurance level EAL3 (or higher) with the additional assurance requirement of an Informal Target of Evaluation (TOE) Security Policy Model (ADV_SPM.1).

An equivalent evaluated trusted operating system may be used. The implementation of a trusted path protects plaintext CSPs and the software and firmware components of the cryptographic module from other untrusted software or firmware that may be executing on the system.

1.4 Security Level 4

Security Level 4 provides the highest level of security defined in this standard. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defenses. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and zeroize CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.
Security Level 4 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that

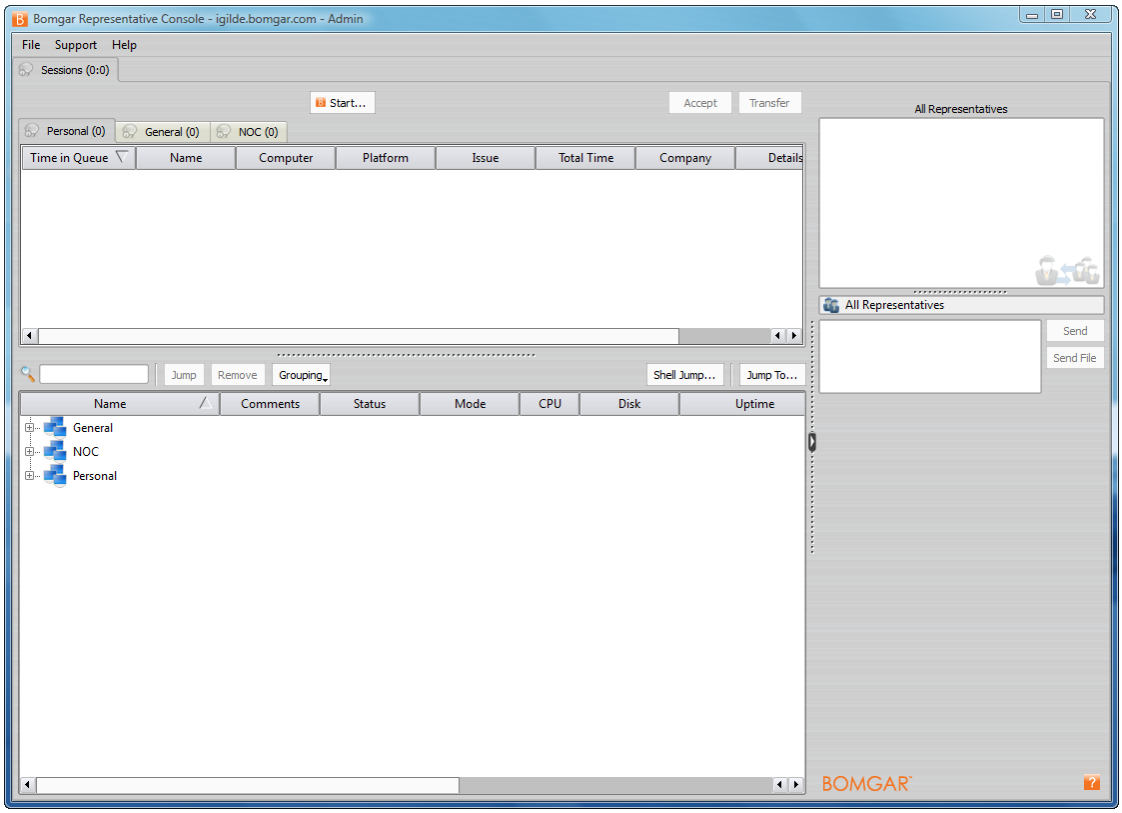
- meets the functional requirements specified for Security Level 3 and
- is evaluated at the CC evaluation assurance level EAL4 (or higher).

An equivalent evaluated trusted operating system may be used.

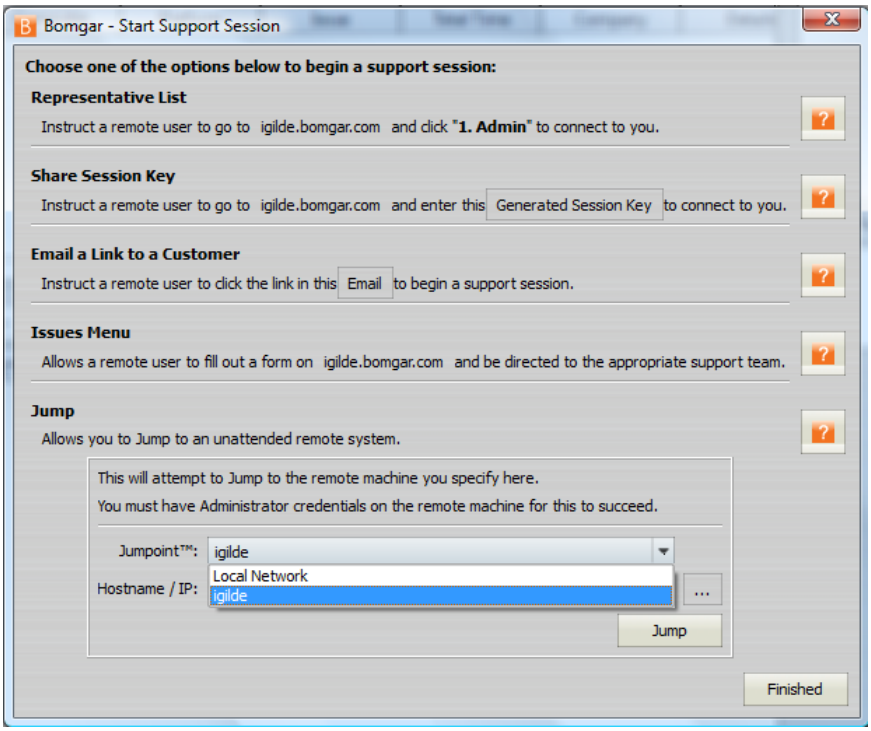
The full documentation of FIPS 140-2 can be found on the following web page:

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

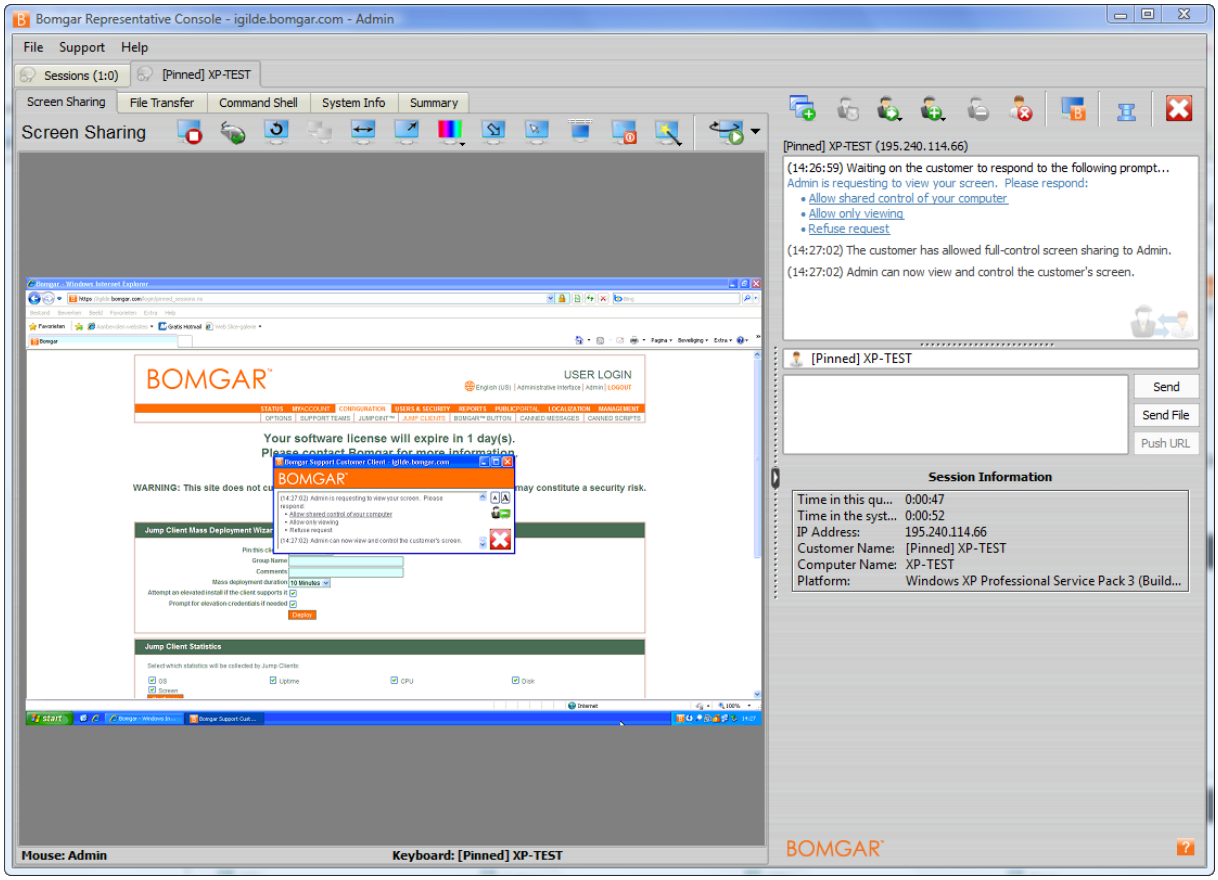
Bijlage 6: Bomgar screenshots



Figuur 15: Bomgar beheerconsole

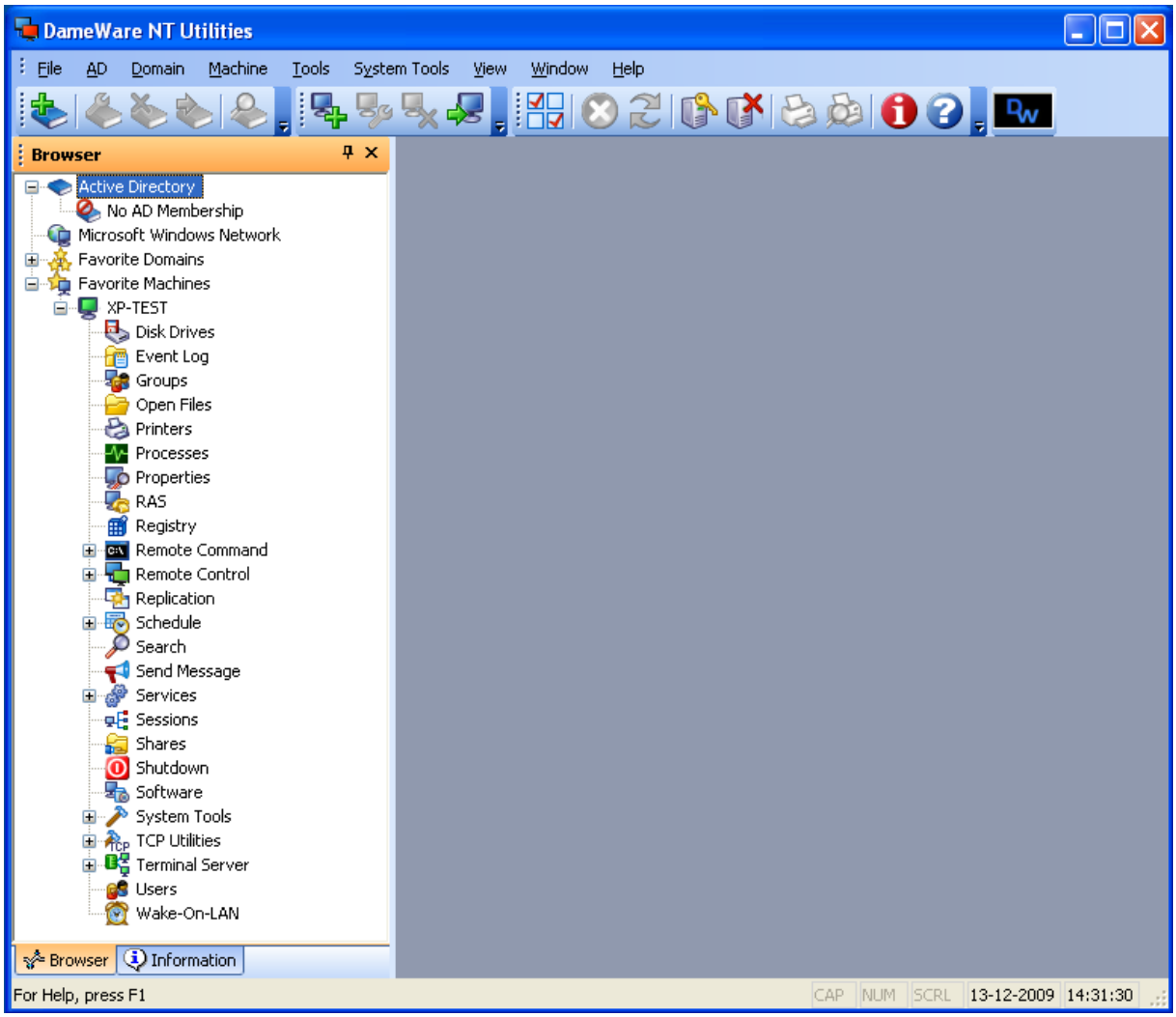


Figuur 16: Bomgar, begin een support sessie



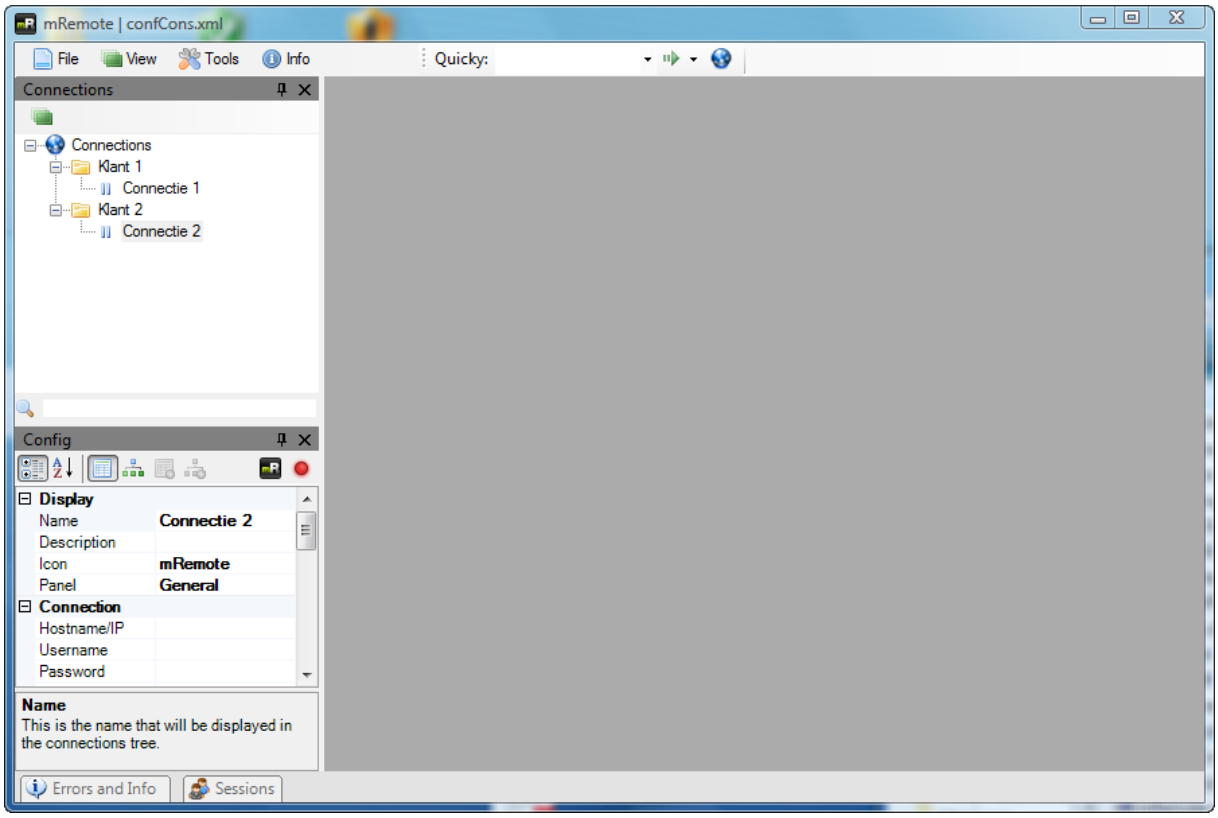
Figuur 17: Een support sessie met Bomgar

Bijlage 7: DameWare screenshots



Figuur 18: DameWare beheerconsole

Bijlage 8: mRemote



Figuur 19: beheerconsole mRemote