

Afstudeerscriptie: de kinderwerkplek



Daan de Boer

Systeembeheer – SV4C

1574031

Daan.deboer@student.hu.nl

04-01-2013

Voorwoord:

Deze scriptie beschrijft de afstudeeropdracht die ik heb uitgevoerd voor ICT Plek b.v, samen met mijn bedrijfsbegeleider Marco van Thiel, docentbegeleider Petra Belgraver en collega's op het bedrijf.

Het doel van mijn afstudeeropdracht is om een advies uit te brengen ter verbetering van de kinderwerkplek; een computer geïntegreerd in een meubel, die kinderen op een remote desktop spelletjes, educatieve software en andere applicaties laat gebruiken.

De kinderwerkplek zit als product nog in de opstartfase; het concept is er, en heeft al interesse gewekt bij diverse scholen, kinderdagverblijven en naschoolse opvangcentra. Ik hoop dat mijn advies het bedrijf zal helpen het product dusdanig te verbeteren, dat de potentiële klanten over de streep getrokken kunnen worden en dat de kinderwerkplek een succesvol product wordt.

Graag wil ik Marco van Thiel bedanken voor de interessante en uitdagende afstudeeropdracht, en zijn begeleiding tijdens het uitvoeren daarvan. Ook wil ik Petra Belgraver bedanken voor haar begeleiding en haar 'elenchos' tijdens het schrijven van mijn plan van aanpak en scriptie; d.w.z. de vele kritische vragen m.b.t. de inhoud en indeling van deze documenten, met als doel me zelf te laten inzien hoe je deze het beste kunt structureren. Hierdoor heb ik veel geleerd. Tot slot wil ik graag mijn collega's op het bedrijf bedanken voor hun gastvrijheid en hulp bij het afstuderen.

Managementsamenvatting:

De kinderwerkplek is een thin client geïntegreerd in een meubel, die via een remote desktop educatieve software, spelletjes en multimedia content aanbiedt aan kinderen op scholen, naschoolse opvangcentra, enz.

Uit feedback van demogebruikers bleek echter dat de werkplekken niet altijd responsief bleven, dat de kwaliteit van de multimedia niet hoog genoeg was, en dat de internetfilter té veel blokkeerde. Het doel van de afstudeeropdracht was om een advies te leveren dat de kinderwerkplek op deze punten kan verbeteren. Dit moet op een schaalbare manier gebeuren, zodat het product bij steeds meer klanten geplaatst kan worden zonder dat dit problemen oplevert.

Om dit advies te kunnen leveren is er onderzoek gedaan naar Microsoft RDS en Citrix XenApp. Hierbij is gebleken dat XenApp het meeste te bieden heeft:

- Op het gebied van responsiviteit is XenApp beter omdat het quality of service op het netwerk ondersteund;
- Daarnaast is XenApp is beter schaalbaar omdat het load-balancing op basis van policies ondersteund, volledige flash- en multimedia redirection heeft, en de zogenaamde 'branch repeater' aanbiedt.

XenApp kan het beste via de 'XenApp web interface' aangeboden worden aan klanten. De kinderwerkplekken kunnen dan via de 'citrix receiver' verbinding maken met de servers. Er kan dan ook via een browser verbonden worden; hierdoor wordt het mogelijk desktops aan te bieden aan thuisgebruikers en gebruikers met mobile devices, mocht dit ooit wenselijk worden.

Om XenApp te gebruiken is voor elke gebruiker zowel een XenApp licentie als een RDS CAL nodig; de kosten hiervan zijn:

<i>XenApp advanced user license:</i>	<i>€265</i>
<u><i>Windows 2008 RDS CAL:</i></u>	<u><i>€67</i></u>
Totaal:	€332

In totaal zal XenApp €332 per gebruiker kosten, zonder initiële kosten.

Mijn advies luidt, in conclusie, om XenApp te implementeren en aan te bieden d.m.v. de web interface.

Inhoudsopgave:

1. Inleiding	6
1.1 De organisatie	6
1.2 Aanleiding.....	8
1.2.1 Gebruikersfeedback	8
1.2.2 Toekomstige ontwikkelingen	8
1.3 Probleemstelling (hoofdonderzoeksvraag) en deelvragen	9
1.4 Doelstelling afstudeerproject.....	9
1.5 Aanpak:	10
1.5.1 Opbouw scriptie:	10
2. Analyse:.....	11
2.1 Huidige situatie	11
2.1.1 Conceptuele weergave.....	11
2.1.2 Technische weergave	12
2.2 Gewenste situatie	14
2.2.1 De gewenste situatie	14
2.2.2 Eisen:.....	16
3. Technisch onderzoek.....	18
3.1 Verantwoording drievoudige structuur van het onderzoek	18
3.2 Pakketten	19
3.2.1: RDS	19
3.2.2: Citrix XenApp:	22
3.3 Protocollen:	25
3.3.1 RDP	27
3.3.1.1 Responsiviteit.....	27
3.3.1.2: Multimedia.....	29
3.3.2 ICA.....	35
3.3.2.1 Responsiviteit.....	35
3.3.2.2 Multimedia.....	37
3.4 Clients:	39
3.4.1 Lokale GPU	39
3.4.2: Lokale decoder	40

3.5: Web filter:	40
3.5.1 Websense:	40
3.5.2 Yoursafetynet:	42
3.5.3 Conclusie:	43
4. Advies	44
4.1 RDS vs. XenApp:	45
4.1.1 Responsiviteit:	45
4.1.2 Schaalbaarheid:	46
4.1.3 Multimedia:	48
4.1.4 Kosten:	48
4.1.5 Eindconclusie:	49
4.2 Architectuur:	49
4.2.1 Clients in verbinding met de servers via een VPN	50
4.2.2 Clients in verbinding met de servers via een web interface (via 'secure gateway' of 'remote gateway')	51
4.2.3 Clients in verbinding met de servers via een VPN; Branch Repeater wordt gebruikt om bandbreedte verbruik te verminderen	52
4.2.4 Conclusie:	53
4.3 Het advies (conclusie):	54
Bronvermeldingen:	55
Bijlage 1: Plan van aanpak:	58
Bijlage 2: Zelfevaluatie:	91
Bijlage 3: Webfilters:	92
Bijlage 4: Proof of concept:	97
Bijlage 5: Vergelijkingsmatrix:	107

1. Inleiding

In dit hoofdstuk wordt het bedrijf beschreven waar de opdracht voor is uitgevoerd, alsmede het product waar het project om draait. Vervolgens wordt de aanleiding, probleemstelling, doelstelling en aanpak van het project beschreven.

1.1 De organisatie

Het bedrijf ICT Plek b.v., opgericht door Marco van Thiel, levert zogenaamde 'kinderwerkplekken' aan basisscholen, buitenschoolse opvangen en kinderdagverblijven. Dit product zit nog in de opstartfase; het plan is om het product de komende periode uit te gaan rollen bij enkele geïnteresseerden, maar het voldoet nog niet aan alle eisen (zie onderstaand hoofdstuk: aanleiding).

De kinderkwerplek is een computer geïntegreerd in een meubel die enerzijds kinderen een veilige en educatieve computeromgeving biedt en anderzijds gebruikersgemak en minimaal onderhoud voor het personeel van de scholen.

Het idee is dat de kinderen veilig kunnen internetten en educatieve software kunnen gebruiken zonder dat de leraren daar moeite voor hoeven te doen (d.w.z. plug-and-play in de meest strikte zin van het woord). Om dit te bewerkstelligen wordt er gebruik gemaakt van 'thin clients' die verbinding maken met de servers van Kinderwerkplek om de kinderen een (remote) desktop aan te bieden.

Op de site¹ wordt het product als volgt beschreven:

"Heeft u een buitenschoolse opvang , kinderdagverblijf of bent u directeur van een basisschool? Bent u op zoek naar een mogelijkheid om uw kinderen op een veilige en educatieve manier gebruik te laten maken van computers en internet? Ziet u op tegen alle technische vragen die dat gaat opleveren? Heeft u ook last van computers die het regelmatig niet doen, of dat er weer een of andere update geïnstalleerd moet worden? Dan bieden wij -de perfecte oplossing voor u:

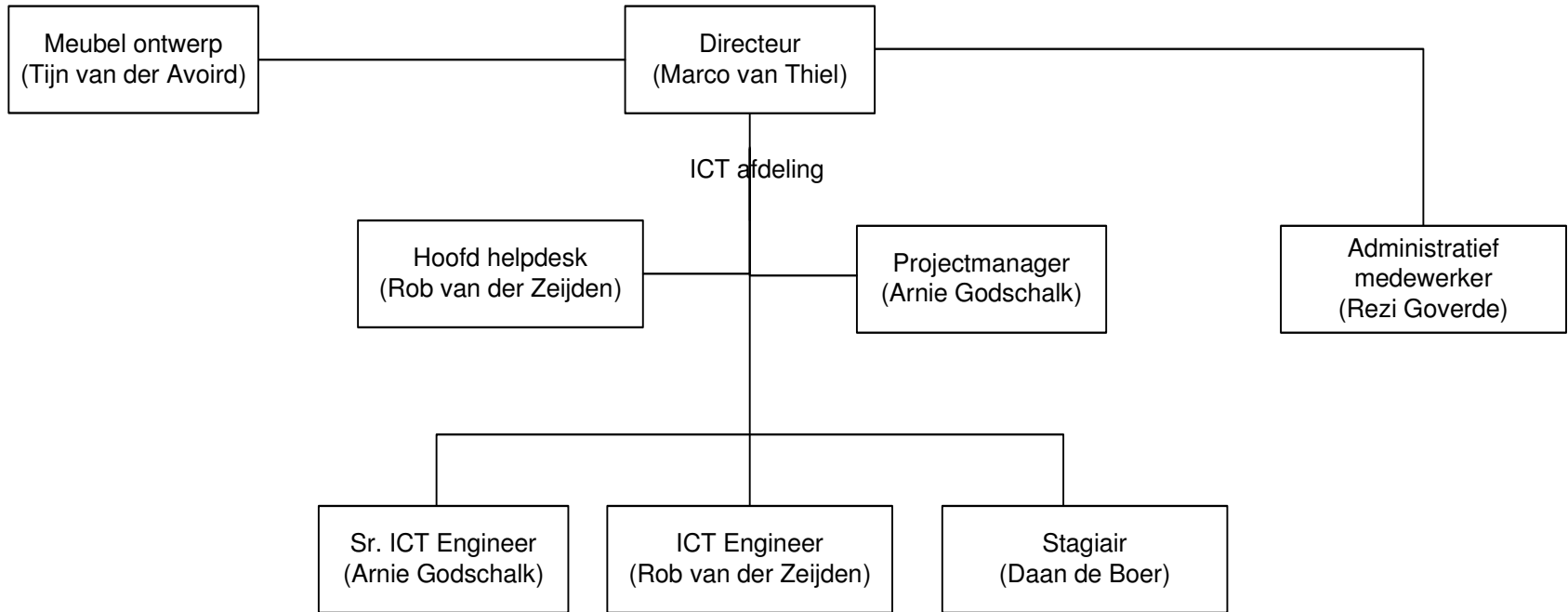
De Kinderwerkplek is een kleurige computerlessenaar voor vier kinderen waarin de computers veilig weggewerkt zijn. De bijgeleverde computers worden door ons geïnstalleerd met educatieve software en een sterke internetfilter. Daarnaast leveren we standaard een doorlopend servicecontract voor het ICT beheer. Hebt u extra wensen? Dan bieden wij speciaal voor u op maat gemaakte uitbreidingsopties.

U en uw medewerkers hoeven zich nooit meer druk te maken over de hard- en de software, alles is geregeld. Het enige wat u hoeft te doen, is de kinderkwerplek aan- en uit te zetten."

¹ <http://www.kinderwerkplek.nl/index.php/component/content/?view=featured&Itemid=101>

Tipdesign B.V. (partner)

ICT plek B.V.



Figuur 1: Organogram

1.2 Aanleiding

1.2.1 Gebruikersfeedback

De kinderwerkplek is een 'thin client' geïntegreerd in een meubel. Deze client maakt een RDP verbinding met 'Remote desktop services' (voortaan RDS) in een datacenter; de gebruiker krijgt vervolgens van RDS een desktop aangeboden. Deze opzet werkt in grote lijnen en heeft al enkele malen proef gedraaid².

Toch wordt er aan een aantal essentiële eisen niet voldaan. Dit is gebleken uit interviews met de doelgroep: de kinderen. Hieronder de conclusie uit een interview met een groep demo gebruikers³:

"De kinderen waren niet tevreden over de snelheid van het internet, het laden van pagina's duurde erg lang en resulteerde soms zelfs in het vastlopen van de computer. Ook vonden de kinderen dat er teveel [internet toegang] afgeschermd werd. [...] Ze gaven aan dat bijvoorbeeld informatie over boeken van Carry Slee die over drugs en geweld gaan ook allemaal afgeschermd werden. De kinderen vonden dat er pakketten voor onderbouw en bovenbouw zouden moeten zijn. Hierdoor is er voor elke leeftijd wat wils."

De aangeboden desktops zijn niet responsief genoeg; daarnaast heeft de webfilter nog niet de juiste balans tussen veiligheid en toegankelijkheid. Ook moet er content te vinden zijn voor de verschillende groepen kinderen. Tot slot is gebleken dat de kwaliteit van de multimedia niet hoog genoeg voor de kinderen⁴.

1.2.2 Toekomstige ontwikkelingen

De verwachting is dat na het verbeteren van de kinderwerkplek er steeds meer werkplekken uitgerold gaan worden. Het is dan belangrijk dat de infrastructuur dusdanig wordt ingericht dat het met het product mee kan groeien.

Naarmate er meer kinderwerkplekken uitgerold worden zal de last op de infrastructuur groeien; deze moet dan zonder de onderliggende architectuur te veranderen opgeschaald kunnen worden (d.w.z., de infrastructuur moet schaalbaar zijn).

In de vorige paragraaf werd vermeldt dat de gebruikerservaring verbeterd moet worden. Het verbeteren van bijvoorbeeld de multimedia zal echter ook extra resources gaan kosten. Het oplossen van de vraagstukken uit de vorige paragraaf zal dus ook op een schaalbare manier moeten gebeuren.

² Op het moment staat er een demo in het 'Tilburg innovation center' (<http://www.t-ic.nl/>).

³ ICT Werkplek B.V.: Operationeel marketingplan; Pieter Kellendonk (2012)

⁴ Ibid.

1.3 Probleemstelling (hoofdonderzoeksvraag) en deelvragen

In de vorige paragrafen kwam de probleemstelling al naar voren; hier wordt hij geëxpliciteerd en geanalyseerd. Omdat het project gericht is op het oplossen van de probleemstelling, moet het duidelijk worden wat deze precies inhoudt.

De probleemstelling is: hoe kan enerzijds de gebruikerservaring verbeterd worden, maar de oplossing anderzijds toch schaalbaar en te beheren blijven?

Deze probleemstelling (oftewel de hoofdonderzoeksvraag) is in verschillende deelvragen op te breken:

De ‘gebruikerservaring’ bestaat uit verschillende zaken; hierbij kwamen de volgende naar voren als problemen:

- **Responsiviteit:** de desktop reageerde niet altijd snel genoeg en liep soms zelfs vast; hoe kan deze bevorderd worden?
- **Internetfilter:** te veel content werd afgeschermd (volgend de kinderen); kan er een filter oplossing komen die flexibel genoeg is om een balans te vinden tussen veiligheid en toegankelijkheid?
- **Multimedia:** de kwaliteit van de multimedia was niet hoog genoeg; hoe kan deze verbeterd worden?

Voor beheer komt het grotendeels neer op één ding:

- **Schaalbaarheid:** Hoe kan de oplossing worden ingericht zodat het met het product mee kunnen groeien, en zodat het kan blijven presteren zelfs als de kwaliteit van de multimedia verbeterd wordt?

1.4 Doelstelling afstudeerproject

De doelstelling van dit afstudeerproject is om een advies te leveren m.b.t. een schaalbare infrastructuur die responsieve kinderwerkplekken aan kan bieden met hoge kwaliteit multimedia en een goede internetfilter.

Dit advies moet gedurende verschillende groeistadia van de kinderwerkplek te gebruiken zijn. Dit betekent dat er in het advies verschillende oplossingen in verschillende prijsklassen naar voren moeten komen. *Met dit advies moet het bedrijf de juiste infrastructuur kunnen kiezen en pakketselectie kunnen uitvoeren.*

Het advies moet het bedrijf op twee manieren helpen:

- Door het verbeteren van de gebruikerservaring de aantrekkelijkheid van het product vergroten, zodat er meer kinderwerkplekken verkocht kunnen worden;
- Zorgen voor een schaalbare infrastructuur zodat het product kan groeien

1.5 Aanpak:

1.5.1 Opbouw scriptie:

Dit document is in vier hoofdstukken (of fases) opgedeeld: inleiding, analyse, onderzoek en advies.

In de inleiding worden de probleem- en doelstelling algemeen uitgewerkt; hier wordt duidelijk waarom het project in het leven geroepen is en in wat voor context de uitvoering ervan plaatsvindt.

In de analyse wordt de probleemstelling verder uitgewerkt door de huidige- en gewenste situatie te schetsen. De doelstelling komt hierdoor duidelijk naar voren, omdat deze als het ware de brug vormt tussen de twee. Het doel van dit hoofdstuk is om de algemene doelstelling uit hoofdstuk één te analyseren zo tot concrete eisen te komen.

Vervolgens wordt in het onderzoek gekeken hoe er aan de eisen voldaan kan worden. Hier vindt de bulk van het (technische) onderzoek plaats. Dit hoofdstuk is descriptief; d.w.z. dat de voor- en nadelen van de verschillende relevante oplossingen binnen het zaakgebied beschreven worden, zonder hier vooralsnog een definitief oordeel over te vellen. Dit gebeurt namelijk in het volgende hoofdstuk: advies.

In het advies wordt uit de verschillende alternatieven uit het vorige hoofdstuk de beste geadviseerd als oplossing voor het probleem.

2. Analyse:

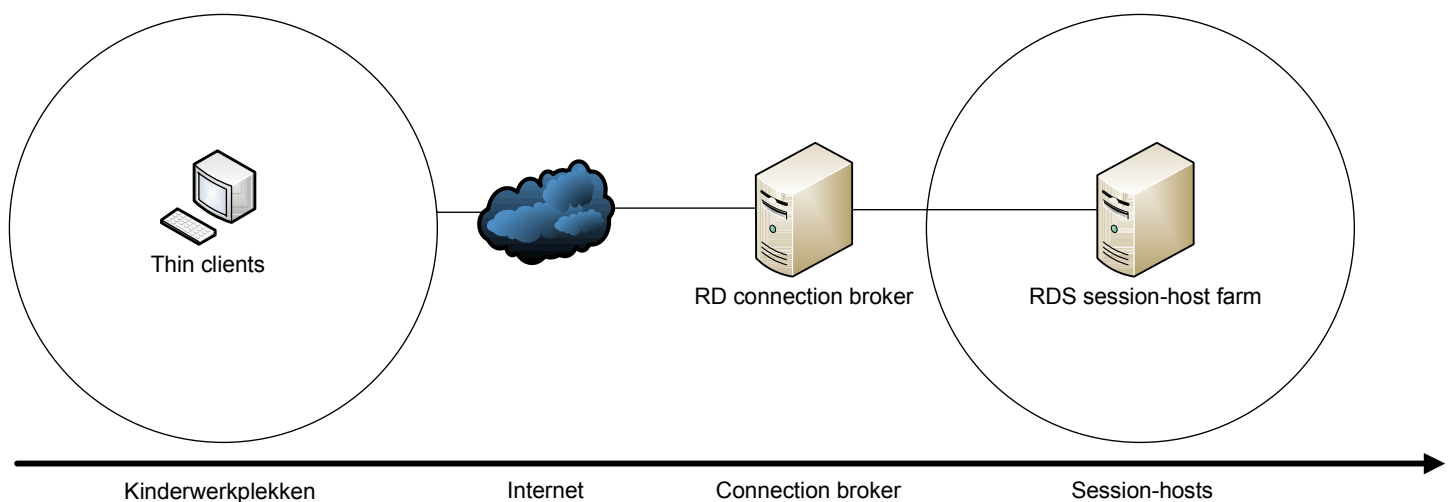
In dit hoofdstuk wordt de probleemstelling uitvoeriger geanalyseerd: eerst wordt de huidige situatie bekeken, vervolgens wordt de gewenste situatie uiteengezet en wordt er een overzichtelijke lijst met eisen gegeven waar de oplossing aan moet voldoen.

Het doel van dit hoofdstuk is om de eisen en de gewenste situatie goed in kaart te brengen, omdat deze het mogelijk maken een advies uit brengen dat relevant is voor het bedrijf. De eisen worden om die reden afgeleid uit interviews met demo gebruikers en uit gesprekken met beheerders⁵. Als er dan een oplossing geadviseerd wordt die aan deze eisen voldoet, zal hij bij de wensen van het bedrijf passen.

2.1 Huidige situatie

2.1.1 Conceptuele weergave

De huidige situatie is hieronder conceptueel weergegeven:



Figuur 2: Conceptuele weergave huidige situatie

De thin clients laden een klein OS (Windows 7 embedded) waarop een RDP client draait. Deze connect met de RDS connection broker in het data center; dit is een server die onder andere de inkomende RDP connecties verdeelt tussen de 'RD session hosts' in de farm. De verbinding makende thin client wordt toegewezen aan een 'session host' en krijgt een desktop te zien.

Op deze desktop zijn (educatieve) spelletjes te vinden en kan gebruik gemaakt worden van internet. De gebruiker wordt d.m.v. policies beperkt tot het gebruiken van geautoriseerde programma's en Windows functies.

⁵ Vgl. 1.2: aanleiding.

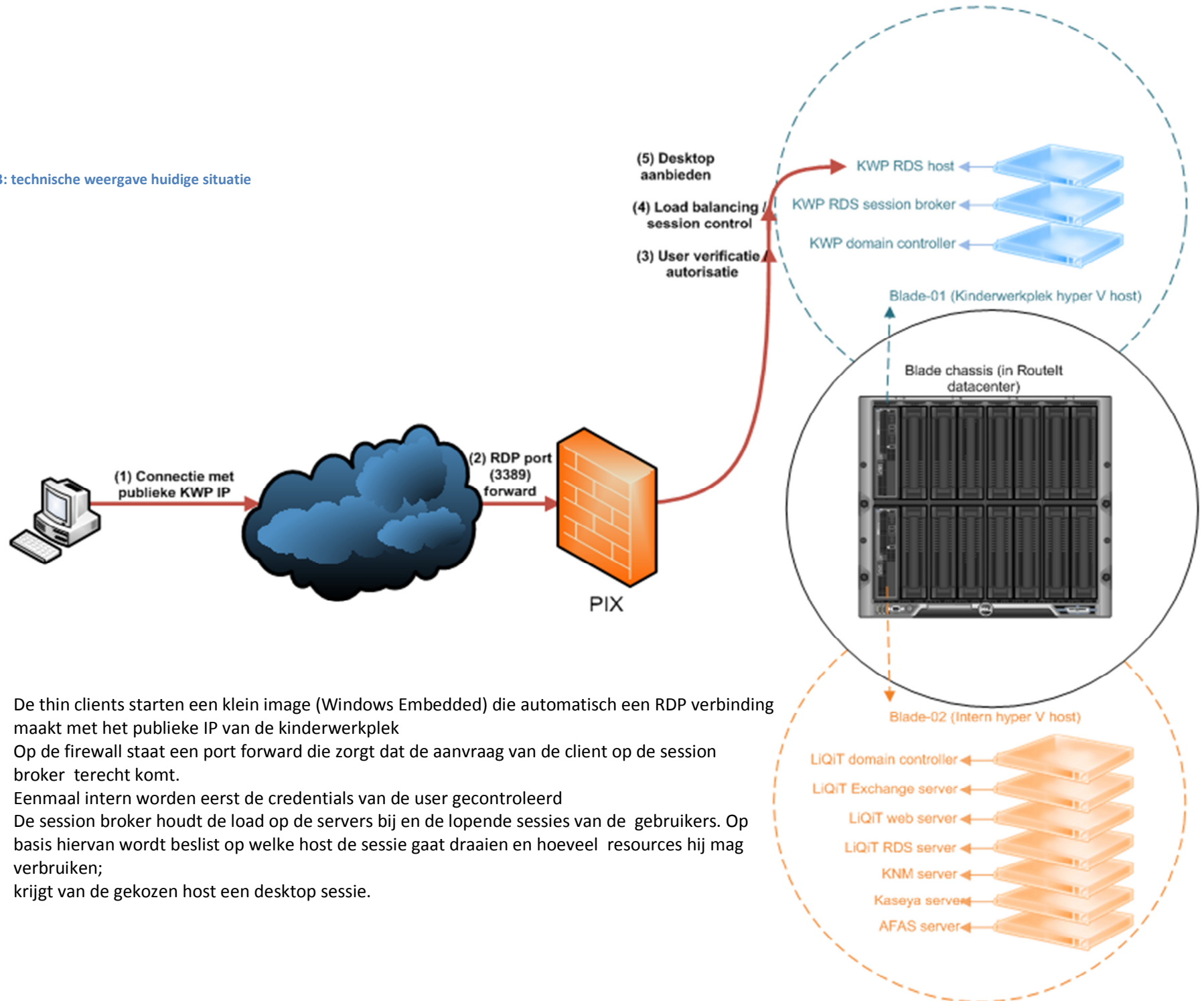
2.1.2 Technische weergave

De servers zijn virtuele machines op Hyper-V hosts (blades in het data center). Er zijn in totaal twee blades: één voor LiQiT (intern) en één voor de kinderkwerplek.

Hieronder een tekening die de Hyper-V hosts en de daarop staande virtuele servers laat zien, alsmede de weg die een client aflegt naar zijn virtuele desktop⁶:

⁶ De stappen zijn genummerd en worden onder de tekening verder toegelicht.

Figuur 3: technische weergave huidige situatie



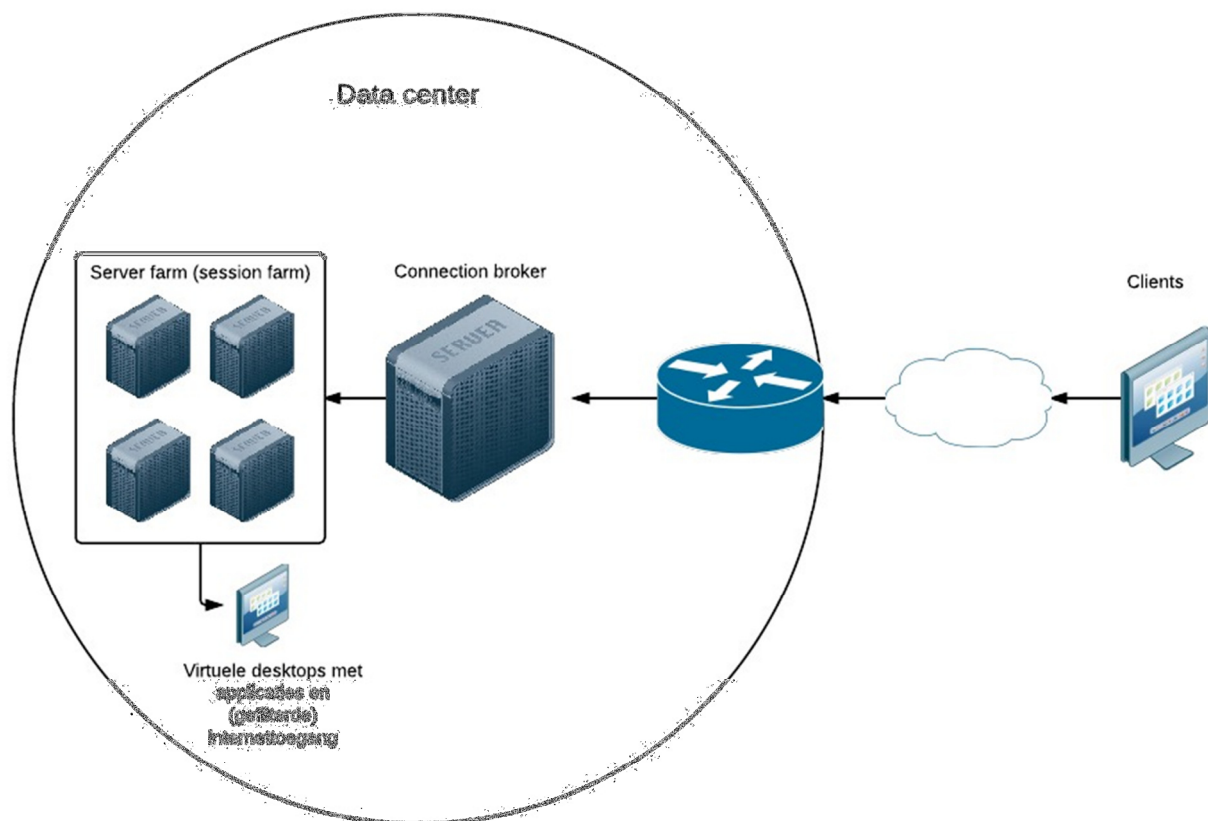
1. De thin clients starten een klein image (Windows Embedded) die automatisch een RDP verbinding maakt met het publieke IP van de kinderwerkplek
2. Op de firewall staat een port forward die zorgt dat de aanvraag van de client op de session broker terecht komt.
3. Eenmaal intern worden eerst de credentials van de user gecontroleerd
4. De session broker houdt de load op de servers bij en de lopende sessies van de gebruikers. Op basis hiervan wordt beslist op welke host de sessie gaat draaien en hoeveel resources hij mag verbruiken;
5. krijgt van de gekozen host een desktop sessie.

2.2 Gewenste situatie

De gewenste situatie komt in grote lijnen overeen met de huidige situatie, de architectuur blijft gelijk: een client maakt connectie met een session broker, die een desktop sessie verschaft (gehost door een farm van 'session-hosts'). De huidige omgeving moet echter zodanig opnieuw worden ingericht, dat de probleemstelling uit het vorige hoofdstuk wordt opgelost. Om dit te bewerkstelligen moet deze algemene probleemstelling vertaald worden naar concretere eisen, die de uitvoering van de opdracht kunnen sturen.

Hieronder wordt eerst een conceptuele weergave gegeven van de gewenste situatie, en worden de verschillende elementen daaruit beschreven (d.w.z. de functie die ze hebben alsmede de eisen die er direct eraan verbonden zijn). Vervolgens wordt een complete eisentabel gegeven, die uitgewerkt is volgens de McCabe methode⁷; hierin is de volledige lijst met eisen overzichtelijk gegeven.

2.2.1 De gewenste situatie



Figuur 4: gewenste situatie

⁷ Vgl. Bijlage 1 van het plan van aanpak voor de gehele analyse van de eisen volgens McCabe; hier wordt enkel het resultaat (de eisentabel) gegeven. Zie verder hoofdstuk 3 (ibid.) voor meer inzicht in het vertalen van de probleemstelling naar specifieke eisen.

Element: Server farm

Beschrijving: De servers in de session-farm hosten de desktops (en / of) applicaties) die de gebruikers uiteindelijk voor zich krijgen.

Functie(s): Hosten van remote desktops
Hosten van remote applicaties

Directe eisen⁸: (21) Active directory integratie voor applicatieaanbod
(41) Applicaties moeten on-the-fly toegevoegd kunnen worden
(43) De server farm moet kunnen worden uitgebreid zonder onderliggende architectuur te veranderen

Element: Clients

Beschrijving: De clients zijn in de kinderwerkplek meubel verwerkt, en maken verbinding met de servers in het datacenter; van deze servers krijgen ze een desktop aangeboden.

Functie(s): Ontvangen van remote desktops

Directe eisen: (48) Clients moeten d.m.v. redirectie last van de servers afnemen

Element: Connection broker

Beschrijving: De connection broker is het toegangspunt voor gebruikers; hij accepteert en verdeelt sessies, en houdt de status bij.

Functie(s): Accepteren / afwijzen van user logins
Bijhouden van sessie statussen (zodat een gebruiker, als hij zijn sessie verliest, deze weer terug krijgt bij het inloggen)
Verdelen van inkomende verbindingen tussen de servers in de sessie-farm

Directe eisen: (21) De logins moeten active-directory geïntegreerd zijn
(44) Load-balancing d.m.v. policies moet mogelijk zijn

Element: Virtuele desktops

Beschrijving: Dit is de desktop die de klant te zien krijgt; hij kan hier applicaties en internet gebruiken.

⁸ Per eis wordt ook het ID gegeven; deze ID is in de eisentabel (2.2.1) vastgesteld en wordt gebruikt om referenties naar eisen te vergemakkelijken.

Functie(s): Toegang tot applicaties bieden aan gebruikers

(Gefilterde) toegang tot het internet bieden aan gebruikers

Directe eisen: (11) Afhankelijk van de groep van het kind moeten verschillende onderwerpen gefilterd worden

(12) Er moet een balans gevonden worden tussen veiligheid en toegankelijkheid voor de kinderen

(14) Op aanvraag moeten bepaalde (combinaties) van termen en specifieke sites toegelaten kunnen worden.

(31 & 32) De desktops mogen niet meer dan 300ms vertraging hebben en indien mogelijk onder de 150ms vertraging blijven

(33) Audio-video asynchroniciteit mag niet boven de 22ms komen

2.2.2 Eisen:

Aan de hand van het onderstaande template zullen de eisen worden verzameld. De eisen zullen worden geselecteerd en ingedeeld aan de hand van de volgende criteria:

- Kerneisen, absoluut aan te voldoen voor het functioneren van het netwerk;
- Features, eisen die nuttig en prettig zijn, maar niet noodzakelijk voor het functioneren;
- Toekomstige eisen, die nuttig zijn in verband met upgrades en revisies;
- Afgewezen eisen, niet nuttige en overbodige eisen.

Het type eis kan Gebruiker (User), Applicatie (App), Host of Netwerk (Netw) zijn. Voor de uitleg van deze indeling zie de methode iAA&D.

De prioriteit loopt van 1 (hoogst) tot 4 (laagst).

Template:

Specificatie van Eisen					
ID/Naam	Type	Beschrijving	Locaties	Status	Prioriteit

Elke globale eis zal een uniek hoofdnummer krijgen (**10, 20**, enz); elke daarvan afgeleide eis krijgt een gesubordineerd nummer onder de eis waaruit hij is afgeleid (**11, 12, 21** enz.).

Specificatie van Eisen						
ID	Type	Beschrijving	Eis	Locaties	Stat	Prio
10	User	Internetfilter	Het internetfilter moet flexibel zijn	Klant	Kern	1
11	User	Internetfilter	Afhankelijk van de groep van het kind moeten verschillende onderwerpen gefilterd worden	Klant	Kern	1
12	User	Internetfilter	Er moet een balans gevonden worden tussen veiligheid en toegankelijkheid voor de kinderen	Klant	Kern	2
13	User	Internetfilter	Aanvankelijk moet veiligheid de meest nadruk krijgen; d.m.v. kinder- en leraren feedback wordt de filter teruggeschoefd.	Klant	Kern	1

14	User	Internetfilter	Op aanvraag moeten bepaalde (combinaties) van termen en specifieke sites toegelaten kunnen worden.	Klant	Kern	2
15		Internetfilter	Chatten op internet moet beveiligd kunnen worden		Kern	2
16		Internetfilter	Op verschillende tijdstippen moeten er andere filters kunnen gelden		Kern	1
17		Internetfilter	De filter moet met tijdsquota kunne werken		Kern	2
18	App	Internetfilter	De filter moet active directory geïntegreerd zijn.	Datacenter	Feature	1
20	User	Applicatie aanbod	Afhankelijk van groep moeten verschillende applicaties aangeboden worden	Klant	Kern	2
21	App	Applicatie aanbod	AD geïntegreerd	Datacenter	Feature	1
22	User	Applicatie aanbod	Applicaties moeten touch-screen ondersteunen	Klant	Feature	3
30	Host	Responsiviteit	De desktops moeten responsief blijven, zelfs bij suboptimale internetverbindingen	Klant	Kern	1
31	Host	Responsiviteit	De desktops mogen niet meer dan 300ms vertraging hebben	Klant	Kern	1
32	Host	Responsiviteit	De desktops moeten indien mogelijk onder de 150ms vertraging blijven	Klant	Feature	2
33	Host	Responsiviteit	Audio-video asynchroniciteit mag niet boven de 22ms komen	Klant	Kern	1
34	Netw.	Responsiviteit	Quality of service moet gebruikt kunnen worden om interactieve data voorrang te geven	Datacenter	Kern	1
40	Netw.	Schaalbaarheid	De infrastructuur moet schaalbaar zijn	Datacenter	Kern	1
41	Netw.	Schaalbaarheid	Applicaties moeten on the fly toegevoegd kunnen worden	Datacenter	Kern	1
42	Netw.	Schaalbaarheid	Storage moet kunnen worden uitgebreid zonder onderliggende architectuur te veranderen	Datacenter	Kern	1
43	Netw.	Schaalbaarheid	De server farm moet kunnen worden uitgebreid zonder onderliggende architectuur te veranderen	Datacenter	Kern	1
44	Netw.	Schaalbaarheid	Load-balancing d.m.v. policies moet mogelijk zijn	Datacenter	Kern	1
45	Netw.	Schaalbaarheid	Aanbieden van complete virtuele desktops (VDI)	Klant	Afgewezen	-
46	Netw.	Schaalbaarheid	Multimedia- en flash redirectie moet mogelijk zijn	Datacenter	Kern	1
48	Netw.	Schaalbaarheid	Clients moeten d.m.v. redirectie last van de servers afnemen	Klant	Feature	2

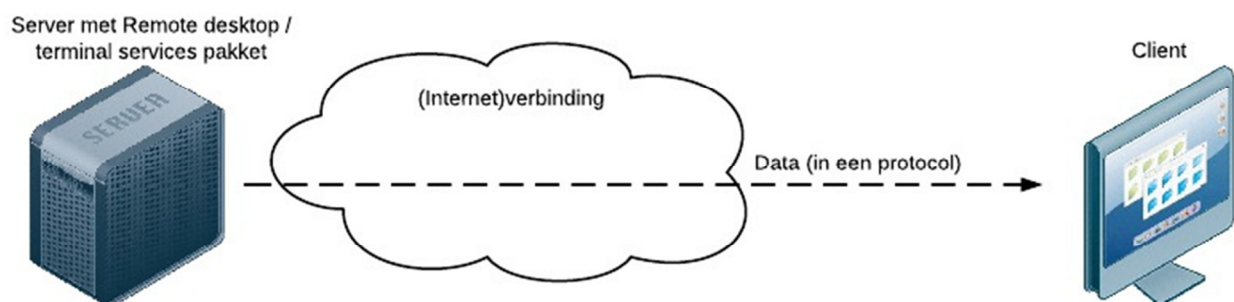
3. Technisch onderzoek

Om een concreter ontwerp te kunnen maken voor de gewenste situatie, moet er eerst onderzoek gedaan worden naar de verschillende mogelijkheden die er zijn. Daarom worden deze hier eerst in meer detail beschreven. Het doel is als het ware de bouwstenen te leren kennen waarmee de oplossing gebouwd kan worden. Als deze dan in het volgende hoofdstuk (hoofdstuk 4: advies) gebruikt worden om verschillende oplossingen te vergelijken en uiteindelijk de beste te adviseren, is het helder waar het over gaat en waarom bepaalde keuzes gemaakt worden.

3.1 Verantwoording drievoudige structuur van het onderzoek

Het onderzoek is onderverdeeld in de volgende onderwerpen: protocollen, clients en pakketten. De reden hiervoor ligt in het 'remote desktop' concept zelf, en in de eisen die hieraan gesteld worden door de opdracht.

Bij het aanbieden van remote desktops aan meerdere clients door een server, zijn er (conceptueel gezien⁹) vier factoren die een rol spelen bij de kwaliteit van de service: het gebruikte pakket, de verbinding, het protocol en de clients:



Figuur 4: remote desktop concept

Van deze vier factoren wordt er één buiten beschouwing gelaten: de verbinding. Volgens eis 30 uit de eisentabel moet de oplossing: “responsief blijven, zelfs bij suboptimale internetverbindingen”. De internetverbinding is—in tegenstelling tot de andere factoren—niet in handen van het bedrijf; het zou niet bevorderlijk zijn voor de verkoop van het product als de klant verplicht zou worden een duurdere internetverbinding aan te schaffen; vooral omdat veel basisscholen juist een langzamere verbinding hebben om kosten te besparen.

Daarom moet er onderzocht worden hoe één of meerdere van de drie overgebleven elementen kunnen bijdragen aan een oplossing die aan de eisen voldoet.

⁹ Uiteraard hangt het ook af van zaken zoals de hardware van de servers; we nemen echter aan dat deze allemaal op orde zijn, en kijken naar de conceptuele opzet van de oplossing, een ‘high-level view’.

Daarnaast wordt er nog gekeken naar een passende webfilter; deze is echter geen essentieel onderdeel van de remote desktop oplossing, maar een onderzoek dat daarnaast loopt.

3.2 Pakketten

Om een advies te kunnen uitbrengen m.b.t. pakketselectie moet eerst alle relevante informatie aanwezig zijn. Dat is het doel van dit hoofdstuk: om alle relevante informatie te verzamelen m.b.t. verschillende remote desktop oplossingen, te weten: RDS en Citrix XenApp.

Met relevante informatie wordt die informatie bedoeld, die kan helpen tot een oplossing te komen die aan de eisen voldoet; van toepassing zijn hier de eisen m.b.t. applicatie aanbod, responsiviteit en schaalbaarheid¹⁰.

Deze informatie moet het advies kunnen onderbouwen. In dit hoofdstuk wordt gekeken welke mogelijkheden elk pakket heeft m.b.t. de eisen, zodat hieruit in het advies een conclusie getrokken kan worden, in feite antwoord gevend op de vraag: gezien de eisen en de mogelijkheden van de pakketten, welke past dan het beste bij de kinderwerkplek?

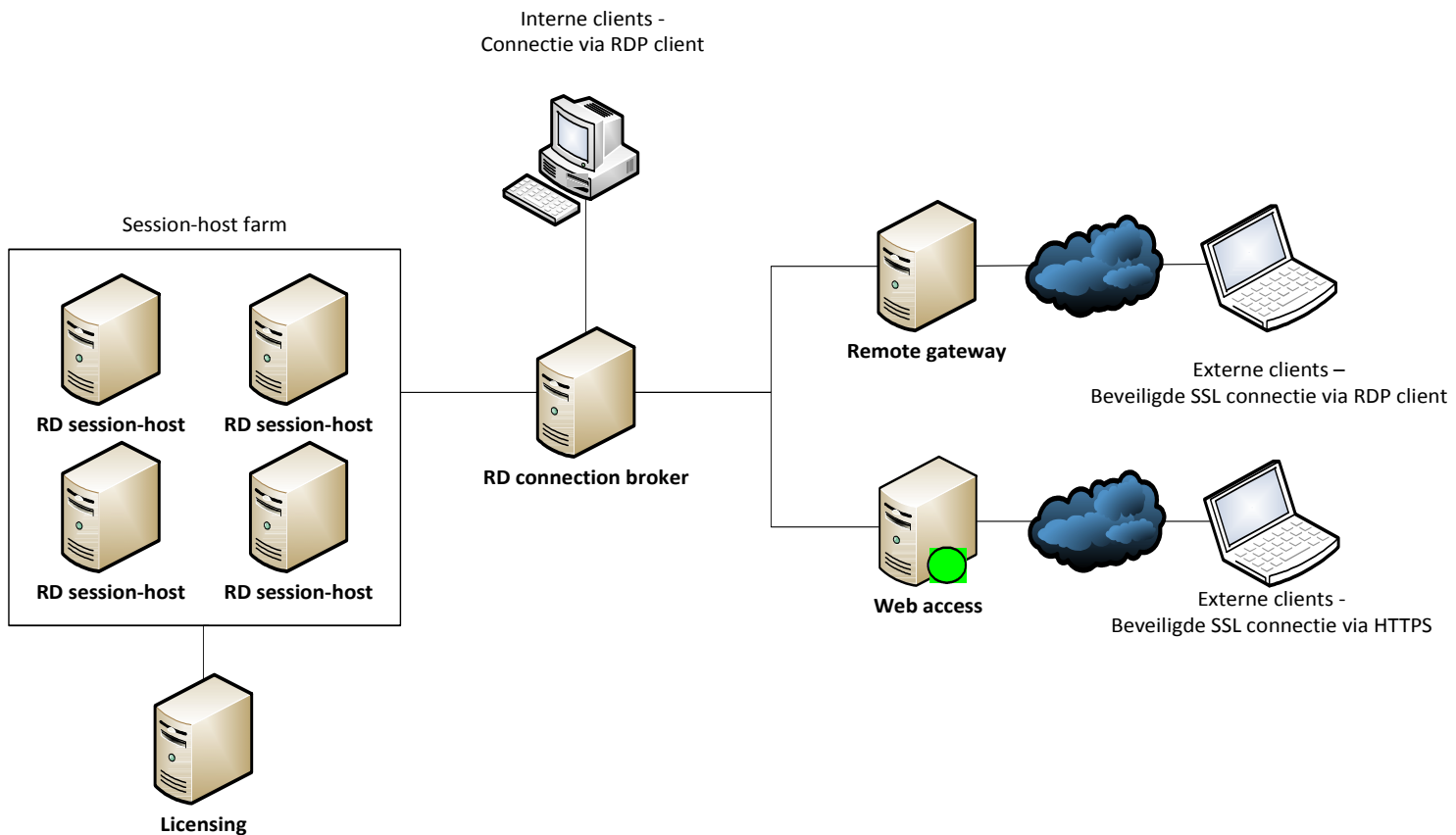
Onder dit hoofdstuk valt ook het derde onderdeel van het onderzoek: protocollen. Dit is omdat de onderzochte protocollen, RDP en ICA, bij de hier onderzochte pakketten horen, RDS en Citrix XenApp respectievelijk.

3.2.1: RDS

RDS staat voor 'remote desktop servies' en is een role op 'Windows server' edities vanaf Server 2008 R2. Hieronder worden eerst de verschillende onderdelen bekeken die het pakket opmaken; vervolgens wordt er gekeken of het pakket aan de verschillende eisen voldoet. Uiteraard is dit geen uitputtende beschrijving van het pakket, enkel voor zover het laat zien of het aan de eisen van de kinderwerkplek voldoet.

RDS kan onderverdeeld worden in vijf onderdelen; door deze onderdelen te beschrijven wordt in grote mate duidelijk wat het pakket kan. Allereerst een illustratie van de architectuur van RDS, vervolgens een beschrijving van de onderdelen:

¹⁰ Zie hiervoor de 20, 30 en 40 eisen uit de eisentabel, bijlage x



Figuur 5: Architectuur RDS

Onderdelen:

- Licensing:

Deze server bevat alle CAL's (client-access licenses). Dit kunnen concurrent- of named CAL's zijn. Concurrent CAL's laten per licentie één gebruiker op dezelfde tijd toe op het systeem. Met 100 concurrent CAL's kunnen er dus maximaal 100 gebruikers op het system tegelijk aangelogd zijn; welke gebruikers dit zijn maakt daarbij niet uit. Named licenties worden daarentegen aan gebruikers gebonden, en staan vervolgens vast. Voor elke gebruiker één CAL.

- RDS Session host:

De 'werkpaarden'. Deze servers draaien de applicaties en desktops waar de gebruikers uiteindelijk mee werken. Door middel van active directory kunnen bepaalde gebruikers en groepen applicaties en desktops toegewezen worden. Als er meerdere session-hosts zijn kunnen deze samengebracht worden in een 'farm'. Deze farm wordt door de 'connection broker' beheerd (zie onderstaande)

- Connection broker

De connection broker biedt de verschillende session-hosts uit de farm als een (logische) eenheid aan bij de gebruiker. Die kan verbinding maken met de connection broker en krijgt vervolgens een desktop of applicatie voor zich die op één van de session-hosts draait. Welke session-host dit is kan bepaald worden door de beheerder (statisch) of d.m.v. load-balancing (dynamisch). Dit wordt doorgaans allen intern gebruikt, omdat een verbinding met de connection broker via poort 3389 gaat, niet via SSL. Zie hiervoor onderstaand: 'remote gateway' en 'web-access'.

Ook houdt de connection broker de sessies van gebruikers bij. Mocht de verbinding van een gebruiker dan onverwachts verbreken, dan wordt deze onthouden sessie bij het herverbinden weer geresumeerd, zodat hij niet al zijn werk kwijt.

- Remote gateway

Remote gateway zorgt voor externe toegang tot de applicaties en desktops via de remote desktop client. Dit betekent dat clients niet langer verbinden via poort 3389 maar een SSL beveiligde verbinding maken via poort 443.

Ook kan er d.m.v. CAP's (client access policies) preciezer bepaald worden welke gebruiker toegang heeft tot welke servers en resources. Daarnaast kan de gateway nog voor enkele andere veiligheidsfeatures zorgen, zoals het alleen toelaten van clients die voldoen aan NAP policies.

- Web access:

Web access heeft ook het doel om externe gebruikers toegang te geven. Dit keer echter niet via de RDP client maar via een browser.

Voldoet RDS aan de eisen:

Hieronder worden de eisen gegeven waar RDS aan moet voldoen. Sommige eisen komen niet hier terug maar onder het hoofdstuk 'protocollen'. De eisen hier zijn vooral eisen m.b.t. features die het pakket moet hebben (e.g. load balancing) en kunnen als zodanig 'zwart op wit' in een tabel beantwoord worden¹¹. De eisen die onderzoek en analyse vergen zijn vragen m.b.t. de protocollen en worden in het volgende hoofdstuk beantwoord.

ID:	Eis:	Voldoet RDS aan de eis?
20	Afhankelijk van groep moeten verschillende applicaties aangeboden worden	Ja; RDS aan verschillende (AD) groepen en users kunnen verschillende applicaties toegewezen worden.
21	AD geïntegreerd	Ja; zie vorige eis.
22	Applicaties moeten touch-screen ondersteunen	Ja, met remoteFX kan dit.
41	Applicaties moeten on the fly toegevoegd kunnen worden	Ja, de service hoeft niet stil te liggen om applicaties toe te voegen.
43	De server farm moet kunnen worden uitgebreid zonder onderliggende architectuur te veranderen	Ja, extra session-hosts kunnen worden toegevoegd aan de bestaande farm zonder dat er iets hoeft te veranderen of stil te liggen.
44	Load-balancing d.m.v. policies moet mogelijk zijn	Ja, d.m.v. het session-broker component.
45	Aanbieden van complete virtuele desktops	Is mogelijk maar niet onderzocht, omdat de eis

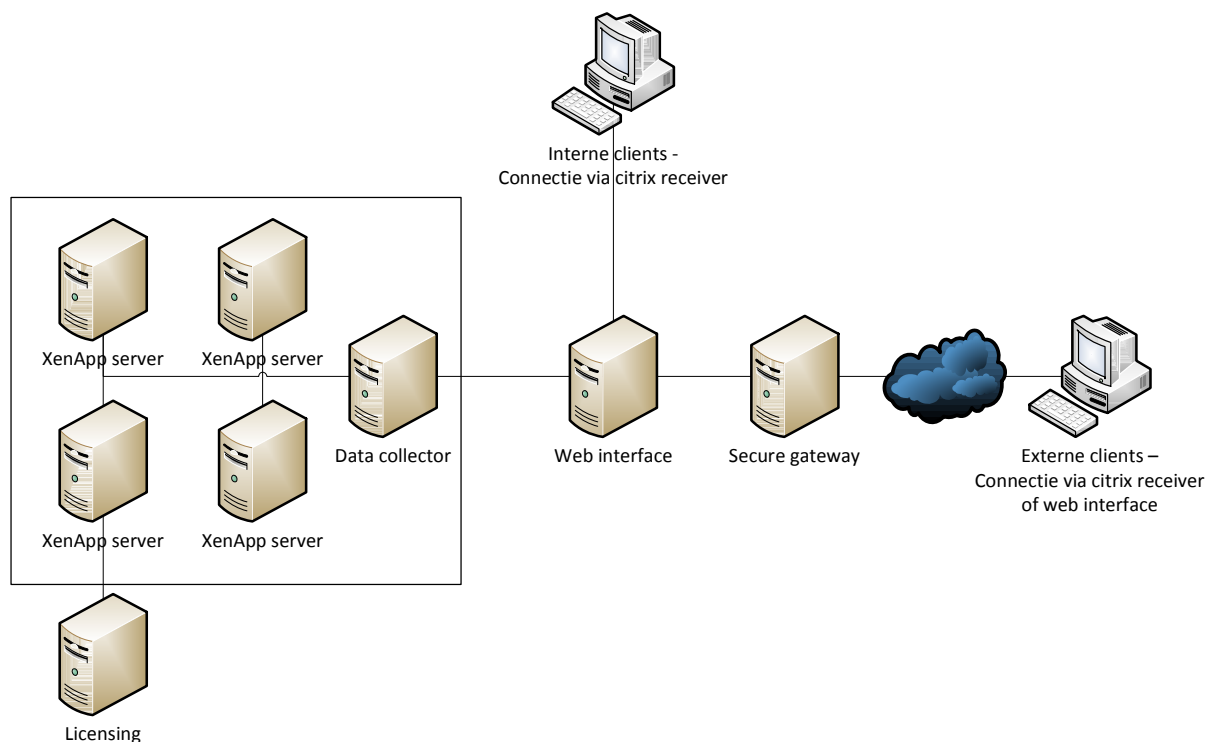
¹¹ De features zijn getest in een testopstelling; zie bijlage 4 proof of concept.

	(VDI)	verworpen is.
--	-------	---------------

3.2.2: Citrix XenApp:

Citrix staat al sinds lange tijd bekend als de 'gold standard' m.b.t. het remote aanbieden van remote desktops en applicaties, en heeft meerdere pakketten in deze markt. Er is gekozen om XenApp te onderzoeken omdat deze het beste bij de use case van de kinderkwerplek past. Een andere mogelijkheid is XenServer; dit pakket kan complete virtuele desktops aanbieden (VDI). Het is echter wel het duurdere pakket, en heeft voor de kinderkwerplek geen meerwaarde omdat er besloten is geen complete virtuele desktops aan te bieden.

Ook voor XenApp worden de architectuur en de verschillende onderdelen daarvan bekeken. Vervolgens wordt er gekeken of het alle features heeft die er geëist worden.



Figuur 6: Architectuur XenApp

Onderdelen:

- Licensing:

Deze server bevat de licenses; net zoals bij RDS zijn er named en concurrent licenses. Naast de Citrix licensing server installeert XenApp automatisch ook de RDS licensing server, omdat voor het gebruik van XenApp zowel Citrix als Microsoft licenses nodig zijn.

- XenApp server:

Host de desktops en applicaties; gelijk aan de 'session-host' in RDS. Applicaties kunnen aan active directory groepen gekoppeld worden.

- Data collector

De data collector is een XenApp server die informatie bijhoudt over ingelogde gebruikers, status van de sessies, hoeveel resources er op elke server vrij zijn, enz. Over het algemeen zijn alle servers data collectors, maar bij een groot aantal gebruikers (en dus veel bij te houden informatie) kan een dedicated data collector gebruikt worden.

- Web interface

Zorgt voor toegang tot de XenApp servers. De web interface heeft twee componenten: web site en service site. De web site geeft gebruikers toegang tot resources via de browser. De service site laat gebruikers verbinding maken via de 'citrix receiver', een software client.

Daarnaast zorgt de web interface voor load balancing. Als een gebruiker zich meldt bij de web interface zal deze de informatie van de data collector(s) gebruiken om te bepalen welke server de meeste resources vrij heeft (of wat voor load balancing policy er ook is ingesteld) en zal de gebruiker naar deze server verwijzen.

- Secure gateway:

Secure gateway beveiligd het verkeer (ICA verkeer) met een SSL certificaat. Als er enkel een certificaat op de website wordt gebruikt, wordt alleen de logon op deze website beveiligd. Door secure gateway te gebruiken wordt *al* het ICA verkeer SSL beveiligd.

Voldoet XenApp aan de eisen:

ID:	Eis:	Voldoet XenApp aan de eis?
20	Afhankelijk van groep moeten verschillende applicaties aangeboden worden	Ja; aan verschillende AD groepen en users kunnen verschillende applicaties toegewezen worden.
21	AD geïntegreerd	Ja; zie vorige eis.
22	Applicaties moeten touch-screen ondersteunen	Ja, met HDX kan dit.
41	Applicaties moeten on the fly toegevoegd kunnen worden	Ja, de service hoeft niet stil te liggen om applicaties toe te voegen.
43	De server farm moet kunnen worden uitgebreid zonder onderliggende architectuur te veranderen	Ja, extra XenApp servers kunnen worden toegevoegd aan de bestaande farm zonder dat er iets hoeft te veranderen of stil te liggen.
44	Load-balancing d.m.v. policies moet mogelijk zijn	Ja, d.m.v. het web interface component.
45	Aanbieden van complete virtuele desktops (VDI)	Niet mogelijk met XenApp, enkel met XenServer; deze eis is echter verworpen.

3.3 Protocollen:

Een protocol is een: “geheel van regels voor de uitwisseling van gegevens”¹². Bij het aanbieden van desktops aan clients zal noodzakelijkerwijs een protocol gebruikt moeten worden om de communicatie tussen beiden te faciliteren.

In dit hoofdstuk wordt uiteengezet waarom onderzoek naar remote desktop protocollen relevant is voor de probleemstelling, en worden de voor- en nadelen van de protocollen op een rij gezet.

Informatie over protocollen is relevant voor de pakketselectie, daar een pakket zich altijd aan één of meerdere protocollen moet committeren om te kunnen communiceren. Door de voor- en nadelen van de verschillende protocollen transparant te maken, wordt direct ook iets belangrijks inzichtelijk over de pakketten die het gebruiken, omdat de limieten van het protocol doorgaans ook de limieten van het pakket bepalen¹³.

Welk protocol gebruikt wordt zal bepalen hoe (en welke) data over de lijn wordt gestuurd. Dit is vooral relevant voor de eisen m.b.t. multimedia, responsiviteit en schaalbaarheid. Daarom wordt per protocol gekeken wat op deze vlakken mogelijk is.

Hierbij worden multimedia en schaalbaarheid samengenomen, daar schaalbaarheid *de facto* tot schaalbaarheid van de multimedia te reduceren is. De redenering hiervoor is als volgt:

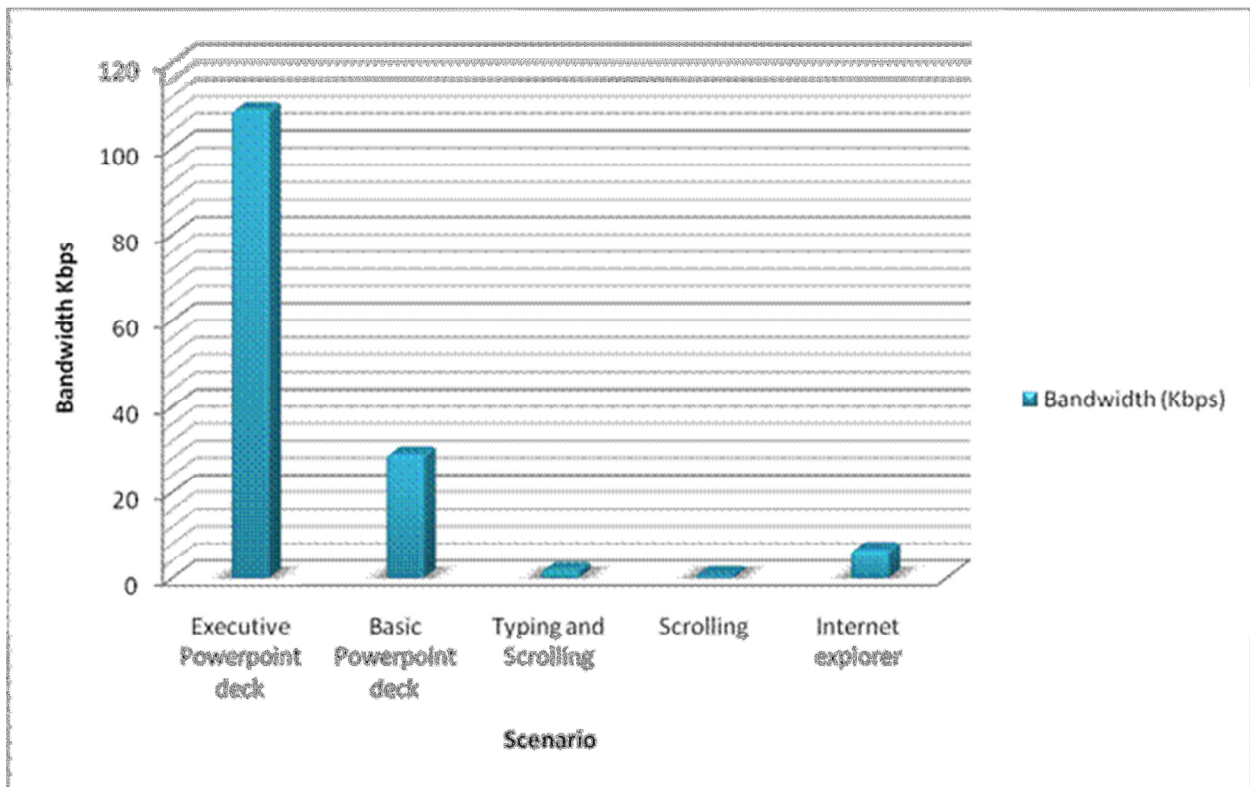
1. Schaalbaarheid in de context van protocollen komt neer op bandbreedte efficiëntie (daar protocollen de regels bepalen m.b.t. communicatie, en deze communicatie data op de lijn is, zal een schaalbaarder protocol minder data verbruiken op de lijn en dus meer communicatie toelaten)
2. Niet-multimedia verkeer gebruikt dusdanig weinig bandbreedte, dat het buiten beschouwing gelaten kan worden
3. Bandbreedte efficiëntie, en dus schaalbaarheid in deze context, komt enkel neer op de efficiëntie van multimedia verkeer

1. volgt uit de gegeven definitie van protocol; 2 wordt op de volgende pagina bewezen; 3. Volgt uit 1 en 2.

¹² <http://www.vandale.nl/opzoeken?pattern=protocol&lang=nn>

¹³ Een willekeurige feature kan als voorbeeld dienen om dit te verduidelijken (laten we zeggen multimedia redirection): als het protocol geen multimedia redirection kent, en een protocol een geheel van regels voor de uitwisseling van gegevens is, bestaan er dus geen regels voor het uitwisselen van gegevens m.b.t. multimedia redirection. Als het pakket zelf deze mogelijkheid wel heeft, zal hij het toch niet kunnen gebruiken, omdat hij op dit vlak niet kan communiceren met de client.

Dat niet-multimedia verkeer slechts triviale hoeveelheden bandbreedte verbruikt, is te zien uit een figuur van microsoft, m.b.t. het bandbreedte verbruik van remote-desktop sessies:



Figuur 7: remote desktop bandbreedte vergelijking

Hier is uit af te lezen dat het gebruiken van internet explorer ongeveer vier 4 kb per seconde verbruikt. Dat dit niet veel is, kan gemakkelijk ingezien worden door deze hoeveelheid door de gemiddelde internetsnelheid in nederland¹⁴ te delen; de uitkomst hiervan laat zien hoeveel simultane sessies de gemiddelde nederlandse internetverbinding aankan: $\frac{8 \text{ mpbs}}{4 \text{ kbps}} = \frac{8000}{4} = 2000$.

De gemiddelde internetconnectie in nederland zou dus 2000 sessies aankunnen die geen multimedia gebruiken, een aantal waar geen basisschool aan zal komen.

Uiteraard zijn dit geïdealiseerde nummers: afhankelijk van het soort websites dat bezocht wordt kan dit nummer stijgen of dalen; toch geeft dit gemiddelde goed weer dat de crux van het schaalbaar maken van de oplossing in de multimedia zit.

Er zal dus zoals gezegd per onderzocht protocol bekeken worden wat mogelijk is m.b.t. responsiviteit en multimedia (en de schaalbaarheid daarvan). Dat wil zeggen dat er gekeken wordt of elk protocol onder de 300ms responsiviteitsgrens kan blijven, zelfs onder suboptimale omstandigheden¹⁵; en of de gewenste multimedia op een schaalbare manier aangeboden kan worden.

¹⁴ De gemiddelde snelheid van internetconnecties in nederland is ~8mbps volgens Akamai (<http://www.akamai.com/stateoftheinternet/>)

¹⁵ Vgl. Eis 31, en eventueel 32 en 33 uit de eisentabel.

3.3.1 RDP

De responsiviteit kan een probleem worden als de beschikbare bandbreedte opdraakt; als er meer data over de lijn moet dan deze aankomst, treedt er congestie op. Een gebruiker zal dan merken dat zijn sessie langzamer reageert, omdat de pakketten niet meer rechtstreeks over de lijn kunnen, maar moeten wachten op andere sessies die ook nog 'in de wacht' staan. Naarmate de situatie verslechterd kan dit ook leiden tot pakketverlies.

Om de responsiviteit consistent te houden zijn er drie aanpakken te overwegen:

- Bandbreedte gebruik verminderen zodat de lijn minder snel volraakt
- Lijn upgraden zodat er meer bandbreedte beschikbaar is, en minder snel volraakt
- Performance bij congestie verbeteren

De tweede optie is zoals gezegd geen mogelijkheid, omdat dit extra kosten voor de klant oplevert. Daarom kijken we wat er mogelijk is om het bandbreedte verbruik te verminderen en de performance bij congestie te verbeteren.

Verminderen bandbreedte verbruik:

Dit zal zoals hierboven al gezegd voor het overgrote deel afhangen van de bandbreedte van multimedia. Dit zal dan ook onder de kop "multimedia" (onderstaand) besproken worden.

Performance bij congestie:

Als de lijn bijna vol raakt zal het vooral aankomen op het prioriteren van bepaalde soorten verkeer. Dé manier om dit te doen is uiteraard 'quality of service'. Hier zal eerst naar gekeken worden:

3.3.1.1 Responsiviteit

Quality of service:

Het is slechts beperkt mogelijk quality of service te doen met RDP. Het is mogelijk prioriteiten te stellen aan verschillende componenten van RDP *binnen* RDS zelf; daarnaast is het mogelijk prioriteit aan RDP als geheel te stellen binnen het netwerk.

Binnen RDS zelf:

De prioriteiten tussen interactieve data(scherm, toetsenbord en muis) en bulk data (file transfer, printen, enz.) kunnen worden aangepast in de registry; dit is dus enkel van toepassing binnen RDS zelf, niet op het netwerk. Dit kan gedaan worden d.m.v. 'display data prioritization'.

Er wordt daarbij onderscheiden tussen twee soorten data: 'Display' en 'channel', d.w.z. interactieve- en bulk data respectievelijk; deze kunnen d.m.v. van registry keys een percentage van de bandbreedte toegewezen krijgen¹⁶. Zo kun je bijvoorbeeld 75% van de bandbreedte toewijzen aan display data om er voor te zorgen dat RDS onder stress nog steeds responsief blijft.

¹⁶ <http://social.technet.microsoft.com/Forums/da-DK/winserverTS/thread/ee61ee0c-2ea6-4cac-8eee-e7fc268d490d>

Op het netwerk:

RDP stuurt alle data over één poort: 3389. Deze kan door quality of service prioriteit krijgen op het netwerk. Hierdoor zal de responsiviteit consistent worden; bij een hoge netwerkbezetting zal RDP voorrang krijgen, en dus veel minder hinder ondervinden van de beperkte bandbreedte.

Omdat al het verkeer over één poort gaat is er echter geen manier voor netwerkapparatuur om onderscheid te maken tussen de verschillende soorten RDP verkeer. Als je RDP voorrang geeft op het netwerk geef je niet alleen interactieve data (zoals scherm-, muis- en toetsenbord informatie) voorrang, maar ook bulk data zoals multimedia, file transfer en printing. Deze kunnen dan gemakkelijk problemen op het netwerk gaan opleveren; vooral omdat het kinderen betreft die veel filmpjes kijken, spelletjes spelen, documenten printen, enz.

Dit wordt een probleem als een netwerk naast RDP nog andere soorten bedrijf kritisch verkeer heeft, zoals duidelijk wordt in het volgende hypothetische scenario:

Voor een bepaald bedrijfsnetwerk is het belangrijkste dat (na VoIP) RDP responsief blijft; daarna komen andere kritische bedrijfsprocessen, daarna pas RDP bulk data en overig verkeer:

QoS Prioriteit:	Soort verkeer:
1.	VoIP
2.	Interactief RDP verkeer
3.	Andere bedrijf kritische processen
4.	RDP bulk verkeer
5.	Overig verkeer

Dit is niet mogelijk met RDP omdat netwerkapparatuur niet kan onderscheiden tussen de verschillende soorten RDP data. Daarom *moet* er gekozen worden tussen één van de volgende scenario's:

QoS Prioriteit:	Soort verkeer:
1.	VoIP
2.	RDP
3.	Andere bedrijf kritische processen
4.	Overig verkeer

RDP heeft nu voorrang boven ander bedrijf kritisch verkeer; het probleem is nu echter dat de bulk data van RDP dit andere verkeer in de weg kan zitten, en dus veel problemen kan opleveren. Om dit te voorkomen kan hiervoor gekozen worden:

QoS Prioriteit:	Soort verkeer:
1.	VoiP
2.	Andere bedrijf kritische processen
3.	RDP
4.	Overig verkeer

Nu ontstaat er echter weer een ander probleem: interactieve RDP data is zeer gevoelig. Als er vertraging optreedt in het scherm, de muis of het toetsenbord, levert dit veel irritatie op bij gebruikers¹⁷. Precies om die reden zou interactief verkeer voorrang moeten krijgen op ander belangrijk verkeer, dat wellicht minder vertragsingsgevoelig is.

Hierdoor loop je in complexere netwerken met meerdere soorten belangrijk verkeer als snel tegen een vorm van *zugwang op*; d.w.z. dat er om de gebruikerservaring hoog te houden quality of service gebruikt *moet* worden, maar dat elke manier om dit te implementeren eigenlijk ongewenst is.

Conclusie

Quality of service met RDP is niet flexibel genoeg. In omgevingen met meerdere soorten belangrijk verkeer wordt het gebrek aan onderscheid tussen interactief- en bulk verkeer binnen RDP een groot probleem. Dit punt moet bij het advies en bij eventuele implementaties in het achterhoofd gehouden worden.

3.3.1.2: Multimedia

RDP was traditioneel bedoelt om servers beheren en via terminal services office- en bedrijfsapplicaties aan te bieden. Grafisch gezien was een 'echte' (fysieke) desktop ervaring niet mogelijk. Om dit wél mogelijk te maken heeft Microsoft in 2008 het bedrijf 'Calista Technologies' overgenomen; een bedrijf dat bezig was remote desktop technologieën te ontwikkelen die de ervaring van een echte desktop kunnen leveren. Deze technologieën heeft Microsoft in 'Windows 2008 server R2 SP1' geïntroduceerd onder de naam 'RemoteFX'. De versie van RemoteFX in Windows 2008 is echter niet bruikbaar voor de kinderwerkplek, omdat deze enkel via LAN werkt; Kinderwerkplek werkt echter vanuit een datacenter over een WAN. Daarom zal noodzakelijkerwijs Windows 2012 server gebruikt moeten gaan worden, die wel WAN ondersteund¹⁸.

Er zal eerst gekeken worden naar wat RemoteFX (nu al) doet; vervolgens naar de veranderingen die in 2012 toegevoegd zijn om RemoteFX via WAN mogelijk te maken.

RemoteFX:

¹⁷ En voldoet zo dus niet aan de responsiviteitseisen: zie eisen 30 t/m 33.

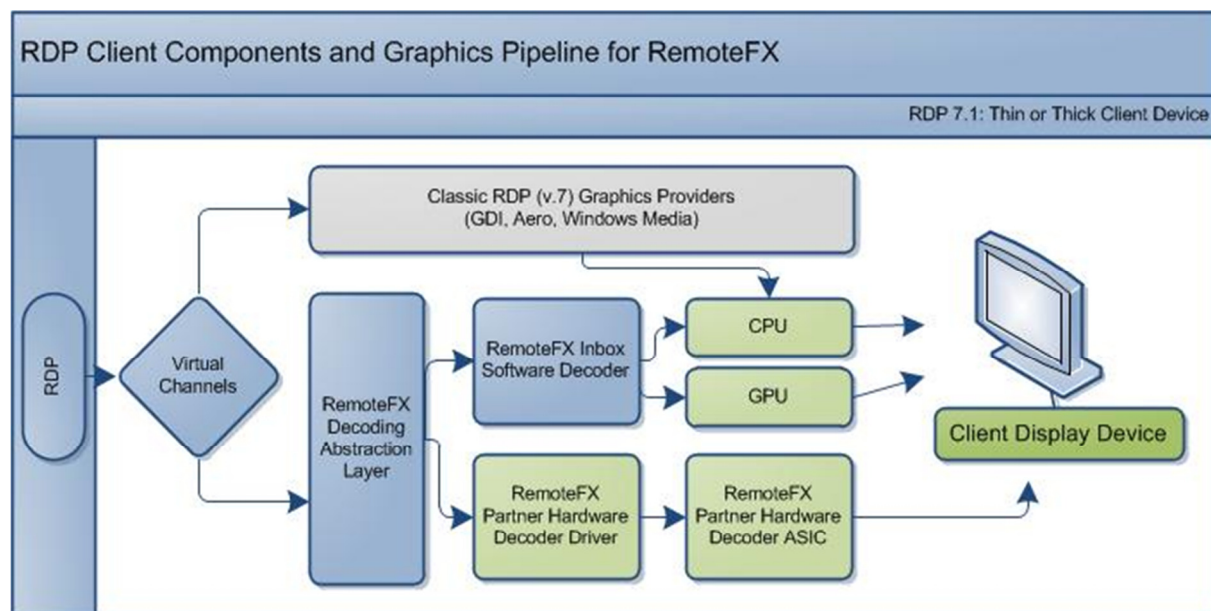
¹⁸ <http://blogs.msdn.com/b/rds/archive/2012/06/13/remote-desktop-services-what-s-new-in-windows-server-2012-release-candidate.aspx>

RemoteFX is een verbetering van het RDP protocol. Het voegt een aantal features toe die gericht zijn op het leveren van een 'full fidelity user experience'¹⁹, gebruik makende van de server GPU en / of CPU, of van die van de client m.b.v. 'client-side computing'²⁰.

Om dit mogelijk te maken is er in RDP versie 7.1 een nieuw soort 'payload' mogelijk gemaakt bij grafische communicatie tussen server en client²¹. D.w.z. dat nieuwe soorten grafische data uitgewisseld kunnen worden. Dit maakt 'real-time' audio en video mogelijk.

Voor 'host-rendering' (het verwerken van grafische data op de server) kan zowel de CPU of een GPU gebruikt worden. Speciaal hiervoor kan een grafische kaart gevirtualiseerd worden die de desktops kunnen gebruiken om grafische data te verwerken. Deze verwerkte data wordt na compressie over de lijn gestuurd²².

Het is ook mogelijk de clients het werk te laten doen; de data wordt dan gecodeerd over de lijn gestuurd zodat de client het zelf kan decoderen. Het onderstaande figuur laat zien hoe:



Figuur 8: RDP client components and graphics pipeline

23

Het figuur is niet gegeven om helemaal te begrijpen, dat ligt buiten de scope van het project; het is bedoeld om enkele features te laten zien die ondersteund worden bij client-side verwerking. In het figuur is een 'Software decoder' te zien; deze kan de CPU en de GPU van de client inzetten om data te verwerken. Daarnaast is er een 'Partner hardware' decoder; deze kan client hardware inzetten die speciaal is gemaakt om grafische data te decoderen (zoals hardware decoders in thin clients).

Samenvattend: de introductie van RemoteFX maakt het mogelijke desktops met hoge grafische kwaliteit te leveren, door gebruik te maken van host- of client-side rendering. Dit werkte tot nu

¹⁹ Microsoft RemoteFX for Virtual Desktop Infrastructure: Architectural Overview [abstract] (<http://www.microsoft.com/en-us/download/details.aspx?id=13864>)

²⁰ Ibid. [RemoteFX overview]

²¹ Ibid. [What's new in RDP In 7.1]

²² Ibid. [RemoteFX for VDI virtual graphics and rendering pipeline]

²³ Ibid. [Clients and Graphics rendering pipeline]

echter alleen op LAN. Dit veranderd zoals gezegd met Windows server 2012; naar deze veranderingen wordt nu gekeken.

RemoteFX for WAN:

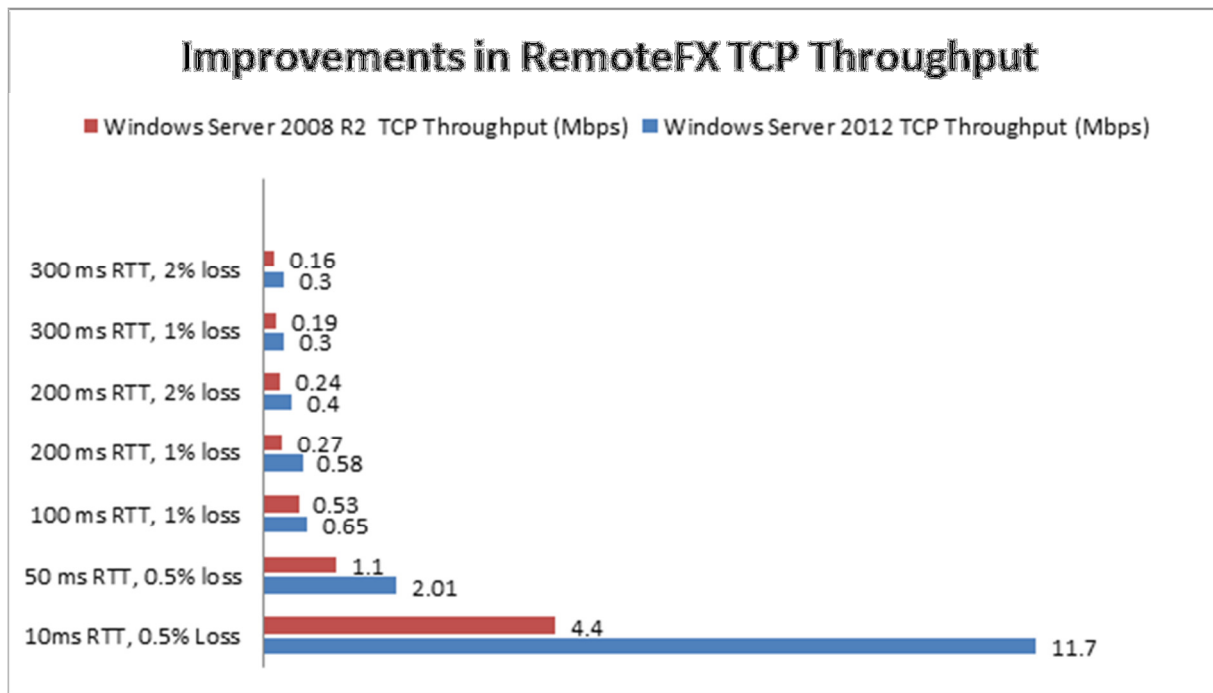
Een van de grote aandachtspunten bij RemoteFX in Windows 2012 was het mogelijk maken van RemoteFX over WAN²⁴. De knelpunten van het gebruik maken van WAN zijn doorgaans: vertraging (latency), packet loss en beschikbare bandbreedte. De verbeteringen zijn gericht op het bestand zijn tegen deze factoren. De belangrijkste toevoegingen zijn de volgende:

Automatic network detection:

Idealiter wordt er zoveel mogelijk data verstuurd zonder 'queuing' (wachtrijen) te veroorzaken op het netwerk (omdat deze vertraging opleveren). Dit is echter lastig te bereiken op een netwerk dat veranderlijk is— zoals WAN. Om dit toch mogelijk te maken zal de nieuwe versie constant de netwerk capaciteit en vertraging in de gaten houden, en op basis van deze informatie zoveel mogelijk data sturen zonder vertraging te veroorzaken. Dit voorkomt aan de ene kant lage responsiviteit (door het sturen van te veel data) en aan de andere kant lage grafische kwaliteit (door het sturen van te weinig data).

Het onderstaande figuur laat de resultaten van deze verbetering zien onder verschillende netwerk condities (RTT = vertraging, loss = packet loss):

²⁴ In microsofts' woorden: <http://blogs.msdn.com/b/rds/archive/2012/08/23/remotefx-for-wan-overview-of-intelligent-and-adaptive-transport-in-windows-8-and-windows-server-2012.aspx>



Figuur 9: Improvements in RemoteFX TCP Throughput²⁵

UDP voor interactieve data:

Voor bepaalde soorten gevoelige data kan het gebruik van TCP een negatief effect hebben; vooral op WAN netwerken. TCP zal niet-aangekomen pakketten opnieuw proberen te sturen; totdat dit nieuwe pakket is aangekomen zal de rest van de data in een wachtrij worden gezet²⁶. De vertraging die dit oplevert is een probleem voor video- en audiokwaliteit, alsmede de responsiviteit van een systeem.

Daarnaast neemt TCP bij packet loss automatisch aan dat dit door netwerk congestie komt, en verlaagd om dit tegen te gaan voor elk verloren pakket de snelheid. Dit is een probleem op netwerken waar packet loss voorkomt die *niet* veroorzaakt wordt door congestie (bijvoorbeeld bij WIFI netwerken die soms kort het signaal verliezen). De snelheid wordt dan constant teruggeschroefd zonder dat dit eigenlijk nodig is (er was immers geen congestie).

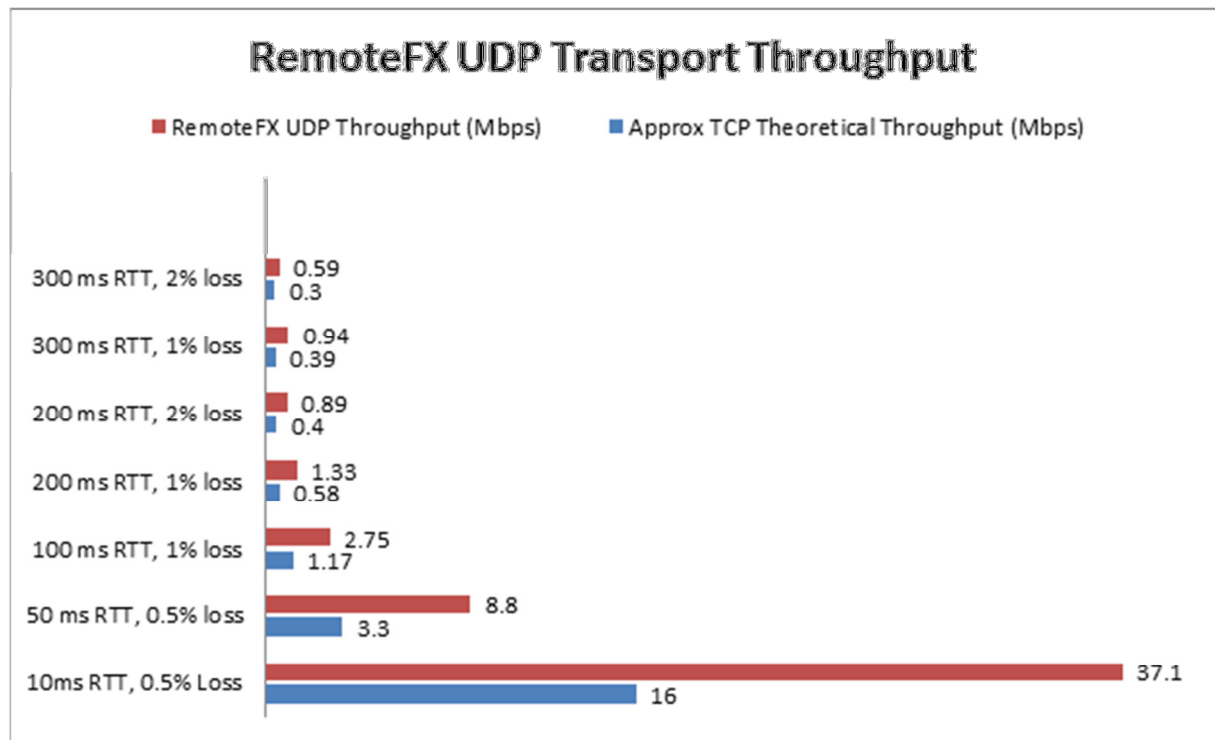
RemoteFX in server 2012 kan met UDP werken om deze problemen te omzeilen. Hiervoor wordt voor sommige doeleinden UDP met 'best-effort delivery' gebruikt (video, audio en interactieve zaken), en voor data waar 'reliability' belangrijk is wordt UDP met 'forward error correction' gebruikt. Dit maakt het mogelijk fouten te herstellen zonder dat dit de vertragingproblemen oplevert die inherent zijn aan TCP²⁷.

Hieronder de performance winst die dit oplevert, gemeten in throughput en vertraging:

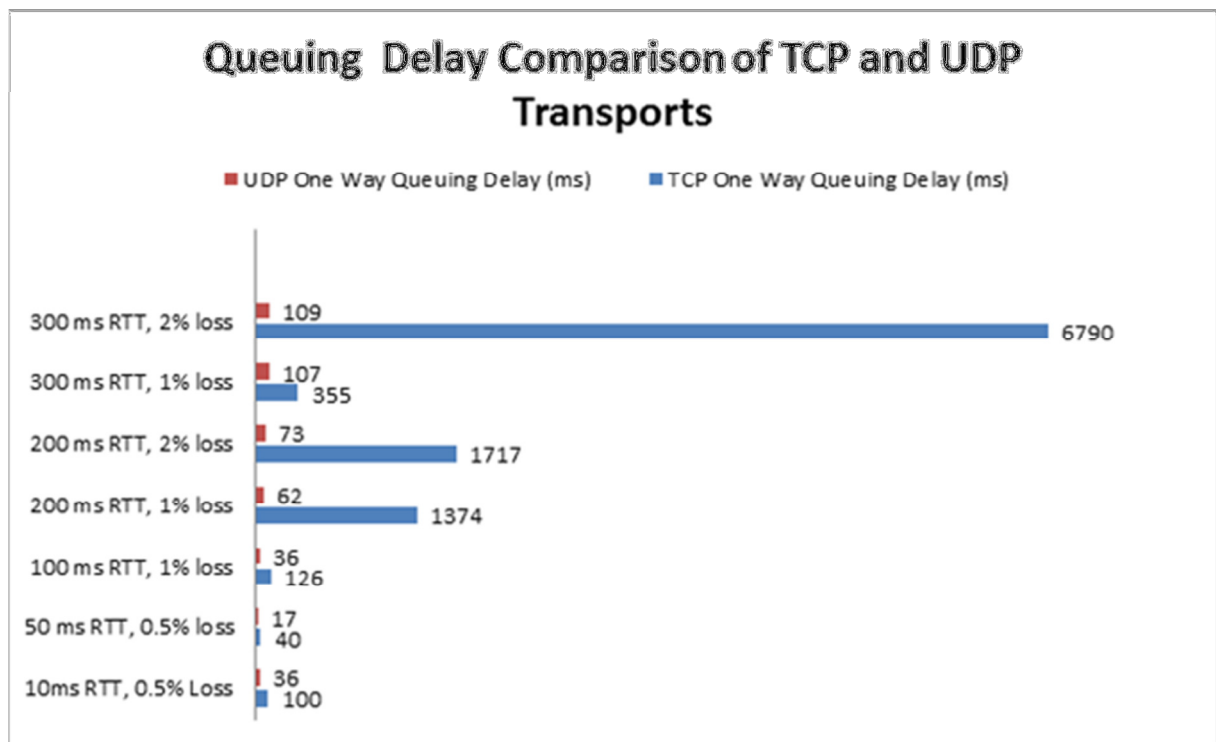
²⁵ Ibid.

²⁶ <http://www.tebyan.net/newindex.aspx?pid=31159&BookID=23760&PageIndex=158&Language=3>

²⁷ <http://blogs.msdn.com/b/rds/archive/2012/08/23/remotefx-for-wan-overview-of-intelligent-and-adaptive-transports-in-windows-8-and-windows-server-2012.aspx>



Figuur 10: RemoteFX UDP Transport Throughput



Figuur 11: Queing Delay Comparison of TCP and UDP Transports

Mediastream (media redirection):

Media redirectie is het over de lijn sturen van een gecodeerde mediastream, die de client vervolgens zelf kan decoderen. Dit was in Windows 2008 enkel mogelijk voor 'Windows media player' content²⁸.

In 2012 wordt een nieuwe techniek geïntroduceerd: Mediastream. Hiermee worden video elementen op het scherm gedetecteerd; deze worden vervolgens gecodeerd met de H.264 codec (de audio met AAC); vervolgens worden ze naar de client gestuurd die ze kan decoderen.²⁹

Dit heeft een aantal voordelen:

- Ondersteund meer als enkel WMP content: o.a. Flash, Silverlight, HTML5 video en Quicktime.
- Minder bandbreedte nodig voor het afspelen van multimedia, omdat de multimedia stream in H.264 over de lijn gestuurd wordt in plaats van volledig gedecodeerd
- Werkt samen met 'automatic network detection' (hiervoor al uiteengezet) om de bitrate en framerate van een video te verhogen of verlagen al naargelang de netwerk omstandigheden

Conclusie:

De verbeteringen voor RemoteFX over WAN zijn veelbelovend en zien er goed uit in theorie. Wel moet er goed gelet worden op het mediastream component. Deze laat zowel de server als de client werk doen (de server codeerd, de client decodeerd). Wellicht levert dit te veel load op bij de server (normaal gesproken zou met redirectie juist alleen de client het werk moeten doen). Dit is iets wat uit het proof of concept moet blijken.

²⁸ <http://blogs.msdn.com/b/rds/archive/2012/08/16/enabling-a-seamless-multimedia-experience-with-remotefx-media-streaming-in-windows-server-2012-and-windows-8.aspx>

²⁹ Ibid.

3.3.2 ICA

Zojuist is onderzocht wat RDP kan op het gebied van responsiviteit en (schaalbare) multimedia. Ditzelfde wordt hier voor ICA onderzocht.

3.3.2.1 Responsiviteit

Quality of service:

Quality of service (QoS) is in de meest recente versie van XenApp een grote stap vooruit gegaan. Het is nu mogelijk volledig netwerk gebaseerde QoS te doen. Om te begrijpen hoe dit bereikt kan worden is eerst wat achtergrond informatie vereist m.b.t. 'virtual channels':

'Virtual channels' zijn virtuele kanalen die voorheen door één TCP connectie heen liepen, en die verschillende soorten data bevatten³⁰:



Figuur 12: ICA Virtual channels

Deze verschillende kanalen konden dan vier verschillende prioriteiten toegewezen krijgen binnen deze ene TCP stream³¹:

³⁰ <http://ctxvm.blogspot.nl/2011/07/ica-virtual-channels.html>

³¹ http://support.citrix.com/servlet/KbServlet/download/23-102-665062/ICA_Priority_Packet_Tagging_FINAL.pdf

Virtual Channel	Default Priority	Description
CTXTW	0	Remote windows screen update data (Thinwire)
CTXTWI	0	Seamless windows screen update data (Thinwire)
CTXCLIP	1	Clipboard
CTXCAM	1	Client audio mapping
CTXLIC	1	License management
CTXVFM	1	Video server video (i.e. not Thinwire video)
CTXPN	1	Program Neighborhood
CTXCCM	2	Client COM port mapping
CTXCDM	2	Client drive mapping
CTXCM	3	Client management (Auto Client Update)
CTXLPT1	3	Printer mapping for non-spooling clients (i.e. WinTerms)
CTXLPT2	3	Printer mapping for non-spooling clients (i.e. WinTerms)
CTXCOM1	3	Printer mapping for non-spooling clients (i.e. WinTerms)
CTXCOM2	3	Printer mapping for non-spooling clients (i.e. WinTerms)
CTXCPM	3	Printer mapping for spooling clients
OEMOEM	3	Used by OEM's
OEMOEM2	3	Used by OEM's

Figuur 13: ICA channel prioriteiten

Hierdoor hebben bepaalde channels prioriteit boven anderen binnen Citrix processen zelf, maar niet op het netwerk omdat het nog altijd één TCP stream is³². Het is dan enkel mogelijk de gehele TCP stream te prioriteren op het netwerk.

Het probleem is echter dat dit niet altijd gewenst is³³. Idealiter krijgt de interactieve data (muis, toetsenbord en scherm) de hoogste prioriteit, terwijl bulk data iets minder krijgt, zodat eventuele andere bedrijf kritische applicaties hier geen last van hebben.

Bij de nieuwste versie van ICA (onder XenApp 6.5) is dit mogelijk; dit wordt ook wel "Multi-stream ICA" genoemd³⁴. Al het ICA verkeer wordt ingedeeld in vier 'klassen', waarvan ieder een eigen TCP stream heeft. De vier klassen zijn:

- Very High Priority (for real-time channels like audio)
- High Priority (for interactive channels like graphics, keyboard, and mouse)
- Medium Priority (for bulk virtual channels like drive mapping, scanners (TWAIN), etc.)
- Low Priority (for background virtual channels like Printing)³⁵

Iedere klasse kan apart geprioriteerd worden d.m.v. een aparte TCP poort. Elke klasse kan daarnaast door de beheerder worden ingedeeld naar believen (d.w.z. de tabel uit figuur 13 kan de beheerder zelf indelen). Dit geeft veel meer flexibiliteit. De prioriteiten op het netwerk van een bedrijf zouden dan als volgt ingericht kunnen worden:

- 1: VoIP
- 2: Interactieve ICA data (muis, keyboard, beeld)
- 3: Eventuele andere bedrijfskritische applicaties
- 4: ICA bulk data
- 5: Overig verkeer

³² What do we mean by enhanced QoS? [<http://blogs.citrix.com/2011/08/25/enhanced-qos-via-multi-stream-ica/>]

³³ Vgl. De nadelen die bij QoS met RDS ondervonden werden (3.3.1)

³⁴ What do we mean by enhanced QoS? [ibid.]

³⁵ How did we achieve enhanced QoS? [ibid.]

Conclusie:

De mogelijkheid om QoS te doen op het netwerk is een groot voordeel voor de kinderkwerplek. Het wordt hierdoor mogelijk de responsiviteit te bevorderen door de interactieve data voorrang te geven op het netwerk, zonder daarbij ander belangrijk verkeer tot last te zijn met hoge prioriteit bulk data; iets wat voorheen—zoals gezegd—wél een probleem was.

3.3.2.2 Multimedia

Het ICA protocol hanteert een set technologieën—samengebracht onder de noemer 'HDX'—om de gebruikerservaring te verbeteren. Veel van deze zijn gericht op het verbeteren van de multimedia ervaring. Hieronder worden de relevante technologieën besproken:

HDX Mediastream:

MediaStream optimaliseert het aanbieden van multimedia content op remote desktops. Het kan zowel server- als client-side de multimedia renderen. De keuze hiertussen kan automatisch gemaakt worden d.m.v. 'adaptive orchestration' (onderstaand behandeld); als het nodig is kan deze ook door de beheerder vastgezet worden.

Van server-side rendering wordt gebruik gemaakt als er gedetecteerd wordt dat de client niet genoeg resources heeft, of als de beheerder dit heeft vastgezet. Voor server-side rendering wordt 'Adaptive display' gebruikt. Deze techniek monitort de kwaliteit en snelheid van de verbinding en past aan de hand daarvan de kwaliteit van de multimedia aan. Naarmate de verbinding verslechtert wordt er meer compressie toegepast. Dit heeft uiteraard als nadeel dat de kwaliteit minder wordt en de processor van de server meer last op zich krijgt³⁶.

M.b.t. client-side rendering kan ICA twee dingen: 'flash redirection' en 'windows media redirection'.

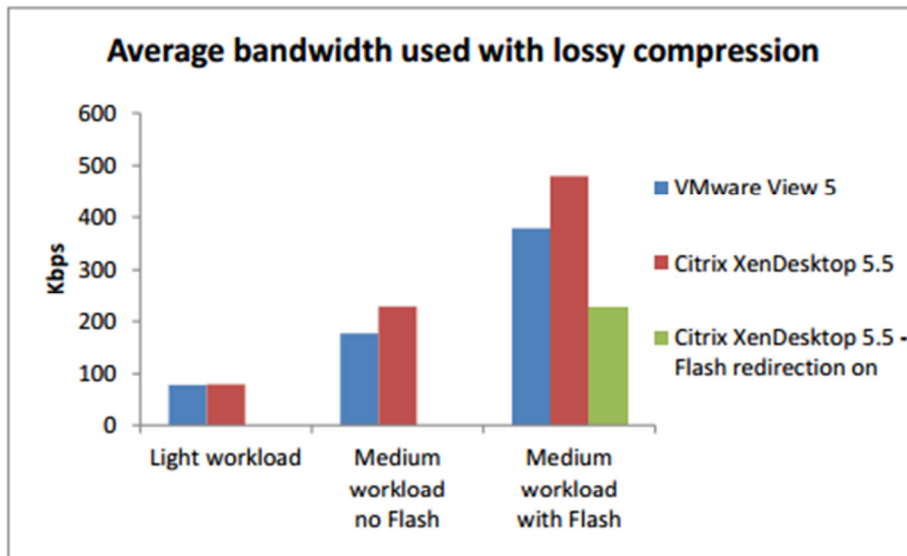
Flash redirection vermindert het bandbreedte gebruik en de server load door flash content op de client te verwerken. Normaal gesproken—zonder flash redirection—wordt het flash filmpje (of spel) op de server geladen en compleet over de lijn gestuurd. Door flash redirection te gebruiken kan de client de flash content zelf verwerken (met de lokale CPU/GPU).

Flash-redirection is op twee manieren mogelijk: 'client-fetch, client-render' en 'server-fetch, client-render'. Wanneer mogelijk wordt de eerste gebruikt. Dit houdt in dat de server de locatie van de flash content aan de client doorgeeft, zodat de client het zelf (met de eigen verbinding) kan downloaden. Dit maakt het afspelen van flash content nog bandbreedte efficiënter³⁷. Als dit niet mogelijk is stuurt de server het naar de client.

Deze techniek kan het bandbreedte verbruik sterk verminderen, zoals te zien is in onderstaande figuren. Zowel tests van Citrix zelf (figuur 14) als van een andere partij (Vmware, figuur 15) laten een sterke reductie aan bandbreedte zien.

³⁶ <http://bramwolfs.com/2012/05/08/adaptive-display-whats-in-the-game-and-do-we-need-to-fine-tune/>

³⁷ Ibid. (p.15)



Figuur 14: bandbreedte besparing met flash redirection 1 ³⁸

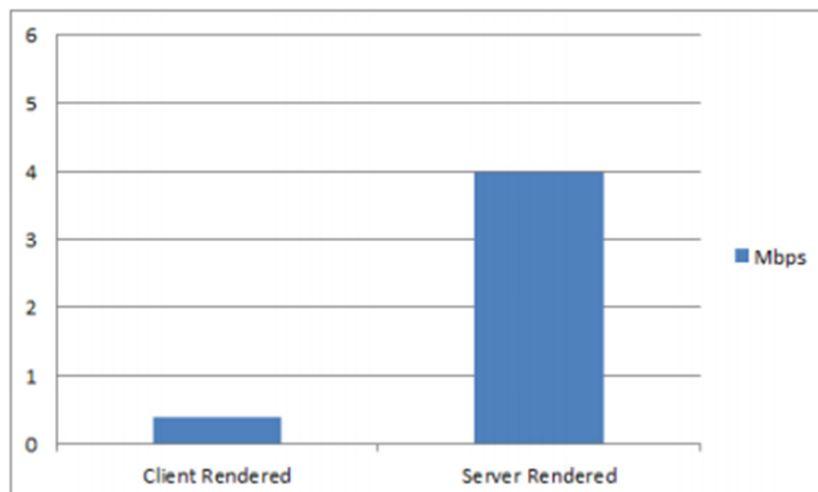


Figure 2: Standard Definition Video Bandwidth with or without Flash v2

Figuur 15: bandbreedte besparing met flash redirection 2 ³⁹

Windows media redirection:

Werkt hetzelfde als flash redirection. Zonder redirection wordt de media door de server gedecodeerd en vervolgens volledig over de lijn gestuurd. Met redirection stuurt de server de media in de originele compressie, zodat de client deze zelf kan decoderen. Dit bespaart zowel server CPU als bandbreedte.

³⁸ <http://www.vmware.com/files/pdf/techpaper/PCoIPvHDXsinglesession03-05-12.pdf>

³⁹ <http://support.citrix.com/servlet/KbServlet/download/29626-102-684449/HDX%20Optimization%20and%20Best%20Practices.pdf>

Wel moeten de codecs voor het bestand zowel op de server als op de client aanwezig zijn. De meest gebruikte codecs worden ondersteund⁴⁰.

Adaptive orchestration:

Deze techniek houdt constant de condities van de verbinding in de gaten. Op basis hiervan ‘orkestreert’ het alle andere technieken. Als de client bijvoorbeeld te weinig processorkracht overheeft om flash content te verwerken, zal het de server aansturen dit te doen; als er te weinig bandbreedte is zal er sterkere compressie gebruikt worden, enz. Alle andere technieken uit HDX worden aangestuurd op basis van de informatie die ‘adaptive orchestration’ verzameld.

De volgende zaken worden hierbij in beschouwing genomen⁴¹:

- “Resources on the end user’s client device running Citrix Receiver;
- bandwidth available on the network connection;
- server resources;
- key application and desktop characteristics.”

3.4 Clients:

De doelstelling is om tot een schaalbare infrastructuur te komen die multimedia ondersteunt. Het probleem is dat naarmate het aantal gebruikers en de kwaliteit van de multimedia toeneemt, het steeds lastiger wordt de kwaliteit consistent te houden. In dit hoofdstuk wordt bekeken wat er client-side ondernomen kan worden om dit probleem aan te pakken.

Er wordt vooral gekeken naar het ‘redirecten’ van grafische data naar de client. D.w.z. dat meer grafische verwerking aan de client-side gedaan wordt. Dit betekent wel dat er enigszins aan het ‘thin-client’ concept moet worden ingeboet, omdat de client resources moet hebben om lokaal data te kunnen verwerken. Dit betreft dan meestal of een grafische kaart, of een media decoder, hoewel het ook enkel met een CPU kan (dit is wel minder efficiënt).

3.4.1 Lokale GPU

Er worden diverse thin- en zero-clients met grafische kaarten geleverd. Deze kunnen dan, afhankelijk van het protocol dat gebruikt wordt, verschillende zaken lokaal afhandelen. Het is niet mogelijk alle grafische berekeningen lokaal af te handelen, enkel wat het gebruikte protocol ondersteunt.

Voor de kinderwerkplek is het belangrijk dat flash filmpjes /spelletjes en multimedia bestanden gebruikt kunnen worden. Als deze door de client afgehandeld zouden worden, zou de serverload en het bandbreedte verbruik verminderd kunnen worden.

⁴⁰ <http://support.citrix.com/article/CTX104912>

⁴¹ <http://support.citrix.com/servlet/KbServlet/download/29626-102-684449/HDX%20Optimization%20and%20Best%20Practices.pdf>

3.4.2: Lokale decoder

Media moet eerst gedecodeerd worden voordat het wordt afgespeeld. Standaard gebeurt dit op de server. Een media bestand wordt gedecodeerd en vervolgens over de lijn gestuurd. Dit betekent extra load voor de server omdat hij moet decoderen en extra bandbreedte verbruik omdat gedecodeerde data groter is dan het originele bestand.

Om dit te voorkomen kan een thin- of zero client gebruikt worden met een ingebouwde media decoder. De server kan dan de multimedia bestanden gecodeerd over de lijn sturen, zodat de client ze vervolgens zelf kan decoderen. Zo wordt er server last en data op de lijn weggenomen.

3.5: Web filter:

Het onderzoek naar de drie hoofdonderwerpen (pakket, protocollen en clients) is nu voltooid. Hier wordt gekeken naar het laatste onderwerp: de webfilter.

Voor de webfilter worden twee oplossingen bekeken: Websense en Yoursafetynet. Deze twee pakketten worden onderzocht op vraag van het bedrijf.

Eerst worden mijn algemene ondervindingen⁴² gegeven m.b.t. deze pakketten; d.w.z. hoe ze in te zetten zijn, hoe gemakkelijk ze geïmplementeerd zouden kunnen worden en hoe beheerbaar ze zijn. Vervolgens wordt er per webfilter eis gekeken of het pakket er aan voldoet. Tot slot wordt er een conclusie getrokken.

3.5.1 Websense:

De webfilter van websense is onderdeel van het gelijknamige pakket, dat een groot aantal modules omvat m.b.t. web-, e-mail- en data security⁴³. Vanaf de installatie is het gelijk duidelijk dat het een zeer complex product betreft; alleen al voor de webfilter zijn er tien verschillende modules te installeren, naast vele mogelijkheden tot integratie met andere firewalls en proxy servers.

Hoe websense ingezet kan worden:

Het overgrote deel van deze modules zijn niet relevant; vooral de integratiemodules niet, daar er geen firewalls of proxies gebruikt worden in de huidige situatie die geïntegreerd moeten worden met de webfilter. De webfilter moet dus 'standalone' gebruikt worden. Hier komt gelijk een probleem naar voren: als standalone filter is het pakket niet flexibel. De enige manier om het in te zetten is om de websense server op een bi-directionele 'span poort' op een switch aan te sluiten, die al het internetverkeer langs ziet komen.⁴⁴

⁴² Ik heb beide pakketten getest; de ondervindingen hiervan komen in dit hoofdstuk terug.

⁴³ <http://www.websense.com/content/TRITON-solutions.aspx>

⁴⁴ Een 'SPAN' poort is een poort die al het verkeer van één of meerdere poorten op de switch doorstuurt naar de device die op de SPAN poort zit. Ook wel 'monitor-' of 'mirroring' port genoemd. Voor meer info zie: http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml

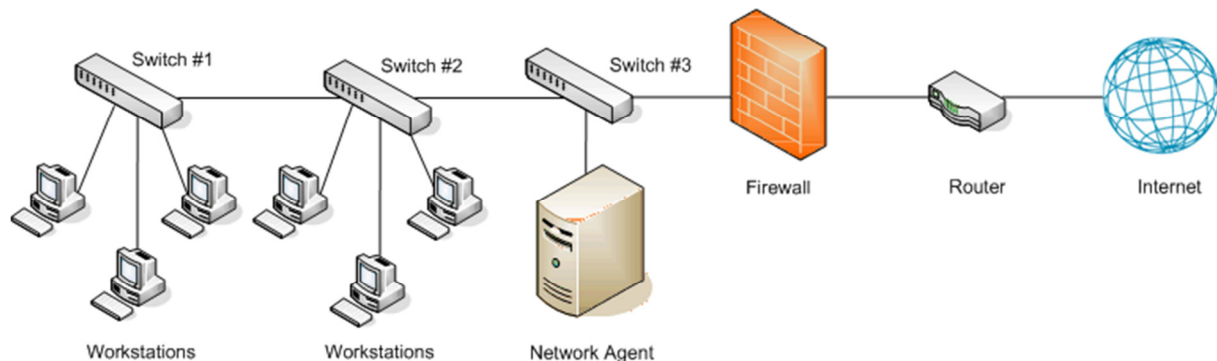
Hoe gemakkelijk de oplossing te implementeren is:

De bovenstaande architectuur vooronderstelt een aparte server (door websense “network agent” genoemd), die aan de switch hangt die al het internetverkeer voorbij ziet komen:

Switched Environment

Requirement: Network Agent must be able to detect traffic coming from all the workstations in the network. Traffic from both Switch #1 and Switch #2 goes through Switch #3 into the firewall.

Solution: The port on Switch #3 to which the Network Agent is connected must be configured to span or mirror the port to which the firewall is connected. All internet traffic that passes through the firewall can then be monitored by the Network Agent.



Figuur 16 Architectuur Websense ⁴⁵

De kinderwerkplek servers zijn echter allemaal virtuele machines op een blade server, die communiceren via een virtuele switch binnen Hyper-V, waardoor het niet mogelijk is de aangeraden architectuur te gebruiken zonder een extra fysieke server te plaatsen (wat veel extra kosten met zich meebrengt). Het is namelijk niet mogelijk SPAN poorten te gebruiken op een Hyper-V virtuele switch op Windows 2008⁴⁶.

Beheerbaarheid:

Het pakket is goed beheerbaar; door de modulaire opzet is mogelijk enkel te installeren wat nodig is. Het instellen van filters en quota's is intuïtief; als de network agent eenmaal geplaatst is en een connectie met de active directory is gemaakt, is het beheren van het pakket niet complex.

Eisen:

Hier wordt enkel de lijst met eisen gegeven en of het pakket er aan voldoet; dit i.v.m. het besparen van ruimte in het hoofddocument. In bijlage 3 kan een uitgebreidere behandeling gevonden worden per eis.

⁴⁵ <http://www.websense.com/support/article/t-kbarticle/Network-Agent-configuration-and-setup>

⁴⁶ Dit wordt pas mogelijk met Windows 2012: http://technet.microsoft.com/en-us/library/jj679878.aspx#bkmk_portmirror

ID:	Eis:	Prio:	Voldoet websense?
11	Afhankelijk van de groep van het kind moeten verschillende onderwerpen gefilterd worden	2	Ja
14	Op aanvraag moeten bepaalde (combinaties) van termen en specifieke sites toegelaten kunnen worden.	2	Nee
15	Chatten op internet moet beveiligd kunnen worden	2	Nee
16	Op verschillende tijdstippen moeten er andere filters kunnen gelden	1	Ja
17	De filter moet met tijdsquota kunne werken	1	Ja
18	De filter moet active directory geïntegreerd zijn.	1	Ja

3.5.2 Yoursafetynet:

Deze webfilter is in grote mate gericht op het veilig maken van internet voor kinderen; het product is aanvankelijk ontwikkelt in gesprek met o.a. kinderen, ouders en schoolorganisaties⁴⁷. De doelstelling van de software is dan ook het internet te beveiligen voor deze doelgroepen, alsmede de software eenvoudig in gebruik te maken, zodat de doelgroepen er mee overweg kunnen.

Hoe yoursafetynet ingezet kan worden:

Deze doelstelling zie je terug in de software; hij is gemakkelijk in te zetten. Yoursafetynet wordt ergens op het netwerk geïnstalleerd en geconfigureerd; vervolgens wordt op de te beveiligen clients een 'agent' geïnstalleerd die de restricties van de server ophaalt, en log informatie terugstuurt.⁴⁸

Hoe gemakkelijk het ingezet kan worden:

De software is gemakkelijk in te zetten. De server software kan op een bestaande kinderwerkplek server geïnstalleerd worden (b.v. de domain-controller); vervolgens kan de client op de terminals-servers (de session-hosts) geïnstalleerd worden. Als een computer dan met een kinder- of groep profiel inlogt op een desktop, krijgt hij de internet restricties mee van de agent .

Beheerbaarheid:

Het programma is zeer goed te beheren; dit komt omdat het de bedoeling is dat leraren en ander personeel de filter ook kunnen beheren⁴⁹. In één interface kun je voor elke gebruiker bepaalde categorieën toelaten of blokkeren, dagdelen toewijzen en quota's instellen. In een twee de kunnen de categorieën zelf aangepast worden of kunnen eigen categorieën gemaakt worden.

Eisen:

Ook de eisen van Yoursafetynet worden in bijlage 3 in meer detail beschreven.

⁴⁷ <http://www.yoursafetynet.com/page/over-ons/over-yoursafetynet/onze-historie/>

⁴⁸ <https://www.yoursafetynet.com/files/modules/content/uploads/downloads/support/yoursafetynet-school-gebruikershandleiding-nl.pdf>

⁴⁹ Beheren enkel in de zin dat ze bepaalde gebruikers bepaalde filters en quota's kunnen toewijzen.

11	Afhankelijk van de groep van het kind moeten verschillende onderwerpen gefilterd worden	2	Ja
14	Op aanvraag moeten bepaalde (combinaties) van termen en specifieke sites toegelaten kunnen worden.	2	Ja
15	Chatten op internet moet beveiligd kunnen worden	2	Ja
16	Op verschillende tijdstippen moeten er andere filters kunnen gelden	1	Ja
17	De filter moet met tijdsquota kunne werken	1	Ja
18	De filter moet active directory geïntegreerd zijn.	1	Ja

3.5.3 Conclusie:

Inzetbaarheid:

Yoursafetynet is veel gemakkelijker in te zetten dan Websense; dit heeft vooral te maken met het feit dat websense gemaakt is voor complexere omgevingen. Waar Yoursafetynet simpelweg ergens op het netwerk geïnstalleerd kan worden waar de agent op de client hem kan bereiken, moet websense op een bidirectionele spanpoort geplaatst worden. Dit betekent, zoals eerder uiteengezet, dat er dan of overgegaan moet worden naar Hyper-V op Windows 2012, of dat er een extra fysieke server geplaatst moet worden. Daarnaast moet er dan nog een switch ingezet worden die bi-directionele SPAN poorten ondersteund; doorgaans niet de goedkoopste. Ook in installatie en beheer is Yoursafetynet eenvoudiger.

Eisen:

Yoursafetynet voldoet aan alle eisen die aan de internetfilter gesteld werden; Websense voldeed slechts aan de meeste. Websense kon niet overweg met *combinaties van* termen; daardoor is het niet mogelijk het 'carry slee voorbeeld probleem' op te lossen. Ook kan Websense geen melding weergeven in chatvensters. Dit is een erg groot nadeel gezien het aantal gevaren die kinderen lopen bij het chatten (cybersex, cyberbullying, etc.). Yoursafetynet kan dit wel; dit heeft te maken met het feit dat dit pakket gemaakt is in overleg met kinderen, ouders en schoolgemeenschappen.

Conclusie:

Yoursafetynet past beter bij de kinderkwerplek dan Websense. Het is gemakkelijker in te zetten, voldoet aan meer eisen, en is bovendien goedkoper.

4. Advies

In dit hoofdstuk wordt het bovenstaande technische onderzoek gebruikt om pakketselectie te doen en te beslissen hoe het pakket ingezet moet worden.

Aan de hand van de vergaarde informatie moet hier duidelijk worden wat de voor- en nadelen van de pakketten zijn, en welke het beste bij de wensen van de kinderkwerplek past. Vervolgens moet er gekeken worden hoe dit pakket het beste ingezet kan worden; d.w.z. hoe de infrastructuur er uit moet komen te zien, en hoe het product aangeboden wordt aan de klanten (m.a.w. de architectuur van de oplossing). Meerdere mogelijkheden worden gegeven en overwogen, waaruit er uiteindelijk één als meest geschikt naar voren zal komen.

De reden dat er in het advies niet direct één oplossing als beste wordt gegeven en dat in plaats daarvan eerst de verschillende mogelijkheden worden bekeken, ligt in de doelstelling die reeds in het plan van aanpak gegeven was; namelijk dat het resultaat van dit project het bedrijf gedurende de verschillende groeistadia van de kinderkwerplek moet kunnen ondersteunen⁵⁰. Omdat het product nog in de opstartfase zit kan er in de toekomst nog veel veranderen; bijvoorbeeld het soort klanten waaraan het product wordt aangeboden, de manier van aanbieden, enz.

De verschillende pakketten en inzetscenario's worden overwogen om hier rekening mee te houden. Per pakket en scenario worden de voor- en nadelen gegeven, en het soort situatie waarin het als beste zou passen. Bij toekomstige veranderingen kan het bedrijf het passende scenario als referentiepunt nemen en de kinderkwerplek aanpassen aan de situatie.

Uiteindelijk wordt er uiteraard wel beslist welk pakket en welke infrastructuur het beste bij de huidige visie van de kinderkwerplek past.

⁵⁰ Plan van aanpak 2.2.3

4.1 RDS vs. XenApp:

In de inleiding zijn vier onderzoeksvragen benoemd: responsiviteit, schaalbaarheid, multimedia en webfilter. Webfilter is reeds behandeld: yoursafetynet wordt hiervoor gebruikt. De anderen zullen hier gebruikt worden om de twee pakketten te beoordelen.

4.1.1 Responsiviteit:

Beide pakketten voldoen uiteraard aan de responsiviteitseisen onder normale omstandigheden; de vraag is hoe goed de gebruikerservaring blijft als de bandbreedte op raakt. Hieronder wordt opgesomd wat beide pakketten kunnen doen in deze situatie, zoals dat naar voren kwam in het onderzoek.

RDS:

De meest voor de hand liggende manier om de responsiviteit consistent te houden is d.m.v. quality of service. Hierdoor is het mogelijk bepaalde soorten verkeer voorrang te geven als het netwerk onder stress staat.

In het onderzoek kwam echter naar voren dat het niet goed mogelijk is QoS op het netwerk te doen met RDS⁵¹. Omdat RDP alles over poort 3389 verstuurd is er voor netwerkkapparatuur geen manier om te onderscheiden tussen interactieve- en bulk data. Het is dus niet mogelijk de responsiviteit te verbeteren door interactieve RDP data voorrang te geven op het netwerk.

Een ander belangrijk onderdeel is 'automatic network detection'⁵². Tijdens de sessie houdt de RDP client automatisch de netwerkcondities bij. Zodra deze verslechteren zal hij de beeld- en audiokwaliteit van de sessie terugschroeven, of extra compressie op de server gaan inzetten. Omdat er nu minder verkeer over de lijn gaat zal de sessie responsiever blijven.

Tot slot kan RDS voor interactieve data UDP gebruiken i.p.v. TCP. Hierdoor treedt er minder vertraging op en wordt er bandbreedte bespaart. Waarom UDP de responsiviteit ten goede komt is in het onderzoek beschreven⁵³.

Citrix XenApp:

D.m.v. van 'multi-stream ICA' is het mogelijk voor netwerkkapparatuur om tussen interactieve- en bulk data te onderscheiden. QoS is dus zeer flexibel in te zetten met XenApp. Door scherm-, muis- en toetsenborddata voorrang te geven zullen sessies responsief blijven, zelfs als het netwerk onder stress staat⁵⁴.

Daarnaast kan XenApp net als RDS de sessie aanpassen afhankelijk van de netwerkcondities (met 'adaptive orchestration'); de beeld- en audiokwaliteit kan terugeschakeld worden, de server kan

⁵¹ 3.3.2.1

⁵² 3.3.2.2

⁵³ 3.3.2.2

⁵⁴ 3.3.3.1

zwaardere compressie gebruiken, en er kan gewisseld worden tussen server- en clientside rendering van multimedia (d.m.v. 'mediastream'⁵⁵).

Ook heeft Citrix een oplossing genaamd 'Branch repeater'; deze kan de sessies responsiever maken door de communicatie tussen client en server zo efficiënt mogelijk te maken.

Conclusie:

Zowel RDS als XenApp kunnen zich aanpassen aan de netwerkcondities. De enige feature die RDS heeft en XenApp niet is het versturen van interactieve data over UDP. Dit is zeker een voordeel, maar weegt niet op tegen de voordelen van XenApp, namelijk flexibele QoS en branch repeater.

De kinderen die aan de kinderwerkplek werken zullen multimedia gebruiken, documenten printen, wellicht files overzetten van de desktop naar hun USB-stick, enz. Hierdoor is het mogelijk dat de bandbreedte opraakt. Als dit gebeurt zal de responsiviteit veel te lijden hebben onder al deze bulk data, *tenzij* er op het netwerk voorrang gegeven kan worden aan de interactieve data. Dat dit niet mogelijk is met RDS is een groot nadeel. XenApp is daarom voor responsiviteit de betere keuze.

4.1.2 Schaalbaarheid:

Er zijn twee soorten schaalbaarheid te onderscheiden in deze context: schaalbaarheid van de infrastructuur en schaalbaarheid m.b.t. bandbreedte. Naarmate er meer kinderwerkplekken komen zullen er meer desktops gehost moeten worden; de infrastructuur zal dan gaandeweg uitgebreid moeten worden (servers, netwerkapparatuur, enz.). Dit moet kunnen gebeuren zonder de achterliggende architectuur van de infrastructuur aan te passen.

Aan de andere kant zal er ook steeds meer bandbreedte verbruikt gaan worden, omdat er meer gebruikers komen die multimedia gebruiken, bestanden printen, etc. Het pakket moet hier efficiënt mee om kunnen gaan. Naarmate er meer bandbreedte gebruikt wordt moet het tegenmaatregelen kunnen nemen. Hierdoor wordt voorkomen dat er telkens meer bandbreedte aangeschaft moet worden, wat voor de klanten erg duur kan zijn, en vaak geen optie is.

RDS:

De desktops en applicaties worden bij RDS gehost door een farm van 'session-hosts'; deze kunnen worden toegevoegd zonder de achterliggende architectuur te veranderen of het systeem stil te leggen⁵⁶.

De 'connection broker' kan load balancing doen tussen de verschillende session-hosts. Als er een nieuwe sessie binnen komt zal de 'connection broker' hem toewijzen aan de server met het minste aantal sessies⁵⁷. Het is niet mogelijk het load balancing gedrag aan te passen; het criterium zal altijd het laagste aantal sessies zijn.

⁵⁵ 3.3.3.2

⁵⁶ 3.2.2.2

⁵⁷ 3.2.2.2

Bandbreedte besparing komt vooral neer op het besparen van bandbreedte bij multimedia. RDS kan dit op twee manieren doen: compressie en redirection. RDS detecteert automatisch video elementen op desktop en comprimeert deze met de h.264 codec; vervolgens wordt de data over de lijn gestuurd⁵⁸.

Deze data wordt vervolgens door de client gedecodeerd (vandaar 'redirection'). Dit bespaart bandbreedte maar zorgt wel voor veel processor belasting. De server moet eerst de video elementen coderen en de client moet het vervolgens decoderen; beide handelingen kosten CPU kracht.

Citrix XenApp:

Ook de XenApp farm kan zonder de architectuur te veranderen en zonder downtime uitgebreid worden. Daarnaast kan XenApp load balancen op basis van policies. Dat betekent dat ook op basis van geografische locatie of het soort user gekozen kan worden. Kinderen in bijvoorbeeld de 'naschoolse opvang' groep, kunnen dan toegewezen worden aan servers die beter geschikt zijn multimedia te behandelen⁵⁹, omdat deze kinderen meer multimedia gebruiken dan kinderen onder schooltijd.

Om bandbreedte te besparen heeft XenApp een aantal opties. Het is mogelijk compressie toe te passen op de data alvorens deze verstuurd wordt. Dit is erg CPU intensief. Het maakt de oplossing meer schaalbaar qua bandbreedte, maar veel minder schaalbaar qua server resources.

Beter is het om 'client-fetch' media redirection te gebruiken⁶⁰. Deze techniek kan bij het afspelen van flash gebruikt worden; de server stuurt dan niets anders over de lijn dan de locatie van de flash content, zodat de client het zelf af kan spelen.

Tot slot is het mogelijk de 'branch repeater' in te zetten. Dit is een apart apparaat dat o.a. compressie toepast en redundante data cached zodat het niet telkens over de lijn gestuurd hoeft te worden. Hierdoor is het mogelijk bandbreedte te besparen d.m.v. compressie zonder de servers ermee te belasten.

Conclusie:

Ook in deze 'categorie' wint XenApp. RDS heeft geen features hier die XenApp niet heeft, terwijl dat andersom wel het geval is: namelijk met load balancing op basis van policies, client-fetch redirection en het bandbreedte verbruik verminderen d.m.v. 'branch repeater'.

Daarnaast is de enige vorm van media-redirection die RDS heeft erg processor intensief; hij moet namelijk alle video elementen zelf gaan coderen. Bij veel gelijktijdige multimedia gebruikers kan dit de server overbelasten.

⁵⁸ 3.3.2.2

⁵⁹ <http://support.citrix.com/proddocs/topic/xenapp6-w2k8-admin/ps-maintain-worker-groups.html>

⁶⁰ 3.3.3.2

4.1.3 Multimedia:

De belangrijkste multimedia criteria zijn die m.b.t. schaalbaarheid; deze zijn hiervoor al behandeld (4.1.3). Noodzakelijk is natuurlijk wel dat de pakketten de benodigde multimedia kan afspelen. Beide pakketten ondersteunen het afspelen van flash, wmv, divx, en andere veel gebruikte formaten, zowel client- als server rendered.

Ook kunnen beide pakketten de kwaliteit van een fysieke desktop leveren in ideale omstandigheden (bijvoorbeeld in een LAN omgeving).

Conclusie:

Beide pakketten ondersteunen het afspelen van de benodigde soorten multimedia en kunnen deze perfect weergeven onder de juiste omstandigheden. De crux zit hem in het afspelen van multimedia in suboptimale omstandigheden

4.1.4 Kosten:

XenApp:

Voor XenApp zitten de kosten puur in de user licenties. Bij een minimum van vijf bestelde user licencies mag XenApp server automatisch gebruikt worden. Er zijn echter niet alleen XenApp licenties nodig, maar ook RDS licenties. Dit komt omdat XenApp onderdelen van RDS gebruikt.

<i>XenApp advanced user license:</i>	€265
<i>Windows 2008 RDS CAL:</i>	€67

In totaal zal XenApp €332 per gebruiker kosten, zonder initiële kosten.

RDS:

Om RDS te gebruiken zijn RDS CAL's (licenties) nodig. Daarnaast zijn er initiële kosten omdat Windows 2012 server gebruikt moet worden; deze is nog niet in het bezit van het bedrijf (daar wordt 2008 gebruikt).

<i>Windows server 2012 standard:</i>	€668
<i>Windows 2012 RDS CAL:</i>	€90

In totaal zal RDS €90 per gebruiker kosten, met initiële kosten van €668. Daarnaast zal er voor elke extra server in de server farm €668 betaald moeten worden.

4.1.5 Eindconclusie:

Uit de vorige conclusies in dit hoofdstuk is gebleken dat XenApp de betere keuze is. XenApp zal onder suboptimale omstandigheden responsiever blijven dan RDS, vanwege de flexibiliteit die het heeft in QoS. Daarnaast zal XenApp minder intensief zijn op de server resources, omdat het pakket om bandbreedte te besparen niet noodzakelijk compressie hoeft te doen (hoewel dit wel mogelijk is).

Daarnaast heeft XenApp in 'branch repeater' een goede oplossing voor grotere klanten. Dit apparaat kan compressie uitvoeren en redundante data cachen, om zo bandbreedte te besparen en de desktops responsief te houden. Dit zal geen impact hebben op de servers omdat het een standalone oplossing is.

Wel moet opgemerkt worden dat al deze voordelen te maken hebben met schaalbaarheid en performance onder suboptimale omstandigheden. RDS functioneert net zo goed als XenApp onder ideale omstandigheden (i.e. verbindingen met meer dan voldoende bandbreedte om het benodigde aantal desktops te draaien).

Dat betekent dat als er nog niet zo veel kinderwerkplekken zijn dat de servers onder zware last komen, én de klanten die ze gebruiken een verbinding hebben die de werkplekken gemakkelijk aankan, XenApp geen meerwaarde heeft. De hogere prijs is in dit geval niet gerechtvaardigd. Dit laatste zal echter zeer waarschijnlijk niet het geval zijn, daar basisscholen, naschoolse opvangen e.d. vaak lage snelheid verbindingen hebben om geld te besparen.

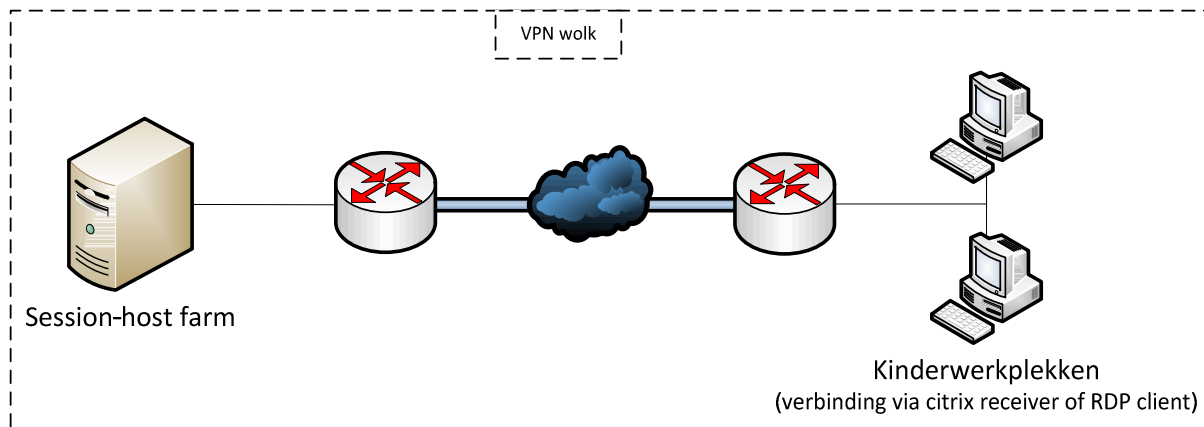
Het bedrijf zal daarom beter voorbereid zijn aan de wensen van de klant te voldoen als XenApp ingezet wordt om de virtuele desktops te leveren.

4.2 Architectuur:

Er worden drie scenario's bekeken:

- Clients in verbinding met de servers via een VPN
- Clients in verbinding met de servers via een VPN; Branch Repeater wordt gebruikt om bandbreedte verbruik te verminderen (alleen mogelijk met Citrix XenApp)
- Clients in verbinding met de servers via een web interface

4.2.1 Clients in verbinding met de servers via een VPN



Figuur 17: VPN opzet

Korte beschrijving:

Het bedrijf levert als dienst aan klanten een VPN wolk, waarmee de klant zijn verschillende vestigingen kan koppelen en ook het beheer gemakkelijker maakt, omdat hij nu in dezelfde wolk zit als zijn beheerder.

Hier kan gebruik van gemaakt worden door de kinderkwerplek. Als de klant namelijk al in de VPN wolk zit, of overgehaald kan worden deze service af te nemen, kan deze wolk gebruikt worden om de clients bij de klant te verbinden met de servers van het bedrijf.

Voordelen:

- Beveiligde communicatie tussen server en clients, omdat het verkeer door een VPN tunnel gaat;
- Een externe gateway is niet per sé nodig, omdat alles 'intern' in een VPN zit;
- Gemakkelijk beheer van de clients door de VPN wolk (veel thin clients hebben management interfaces om images e.d. te beheren, deze kan dan via VPN benaderd worden)
- Veiliger omdat de servers niet direct aan het internet hangen

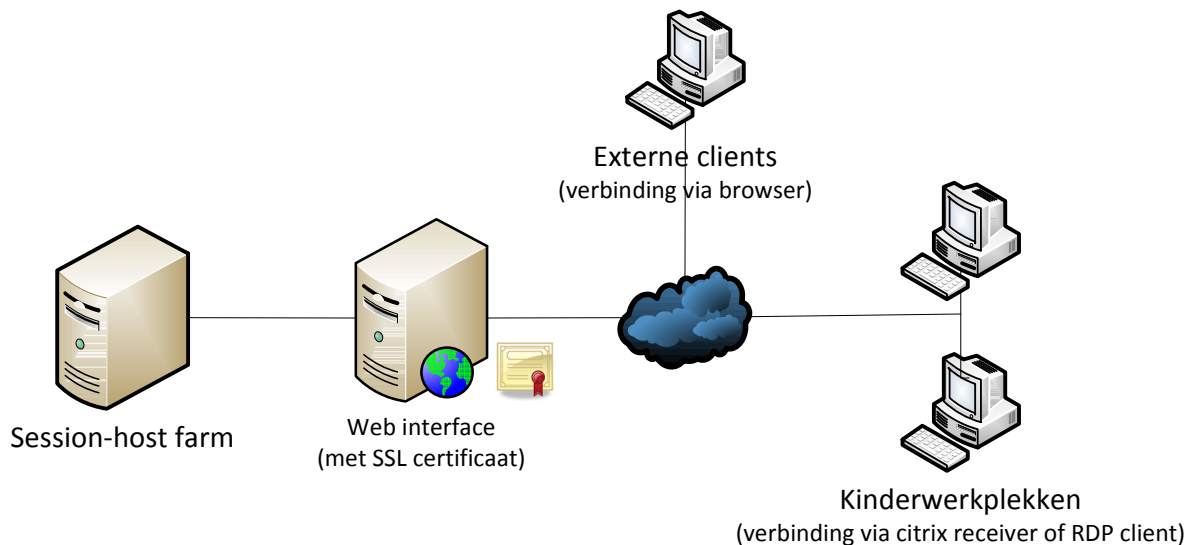
Nadelen:

- Als de klant nog geen VPN heeft zal deze afgenomen moeten worden; het is niet zeker of elke klant daarop zit te wachten (vanwege de extra kosten);
- Geen externe toegang via het internet

Wanneer in te zetten:

Deze oplossing is in te zetten als alle klanten binnen de VPN gebracht kunnen worden. Door de VPN verbinding kunnen desktops aan de klant aangeboden worden, en kunnen de clients beheerd worden op afstand.

4.2.2 Clients in verbinding met de servers via een web interface (via 'secure gateway' of 'remote gateway').



Figuur 18: web interface opzet

Korte beschrijving:

Het is ook mogelijk de clients d.m.v. HTTPS te laten verbinden. Er wordt dan een 'gateway' server opgezet (bij RDS 'remote gateway', bij XenApp 'secure gateway'), die verbinding via een web browser of via een software client toelaat ('RDP client' en 'Citrix Receiver' respectievelijk).

Deze verbinding wordt dan—beveiligd met een SSL certificaat—via HTTPS (op poort 443) tot stand gebracht.

Voordelen:

- Het is niet nodig klanten op te nemen in de VPN-Wolk; dit kan een voordeel zijn als de klant dit niet wilt;
- Verbindingen tussen server en clients worden versleuteld d.m.v. SSL;
- Voor iedereen toegankelijk via internet; kan een voordeel zijn als de kinderkwerplek ooit op internet (aan b.v. thuisgebruikers) aangeboden gaat worden;

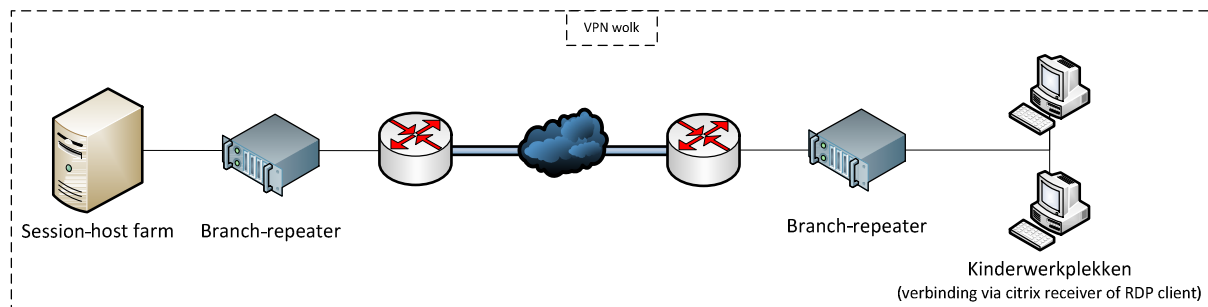
Nadelen:

- Geen simpele manier om thin-clients te beheren, zoals dat in de VPN kan;

Wanneer in te zetten:

Als klanten niet in de VPN willen, of als de kinderkwerplek niet alleen als fysieke meubel maar ook via internet aangeboden moet worden (bijvoorbeeld aan thuisgebruikers).

4.2.3 Clients in verbinding met de servers via een VPN; Branch Repeater wordt gebruikt om bandbreedte verbruik te verminderen



Figuur 19: Branch repeater opzet

Korte beschrijving:

Deze opzet is identiek aan de eerder beschreven VPN opzet. Het verschil is dat er zowel op de server- als op de klantlocatie een zogenaamde 'branch repeater' komt te staan. Dit is een fysieke of virtuele toepassing die gemaakt is om de gebruikerservaring via WAN te verbeteren. Deze oplossing is enkel van toepassing als XenApp gebruikt wordt, daar 'branch repeater' een product van Citrix is en Microsoft geen soortgelijke oplossing heeft.

De belangrijkste manieren waarop 'branch repeater' de performance op WAN verbeterd zijn de volgende:⁶¹:

- Data compressie: data wordt niet volledig over de lijn gestuurd maar gecomprimeerd om bandbreedte te besparen. Dit heeft geen impact op de performance van de servers omdat branch repeater een apart apparaat is.
- Data de-duplicatie: veel voorkomende data patronen (bijvoorbeeld veel voorkomende protocol headers e.d.) worden gecached; de data hoeft dan niet meer verstuurd te worden, enkel een sein dat de gecachte data opgeroepen moet worden
- Protocol acceleratie: veel bekende protocollen—o.a. TCP, HTTPS en NFS—worden efficiënter gemaakt door het aantal 'round trips' per transactie te verminderen. D.w.z. zoveel mogelijk data in zo weinig mogelijk berichten sturen.

Voordelen:

- Minder bandbreedte verbruik
- Responsievere applicaties
- Verbeterde multimedia kwaliteit

Nadelen:

- Extra kosten: er moeten twee 'branch repeaters' komen
- Single point of failure: als de 'branch repeater' zo cruciaal is dat zonder dit apparaat de gebruikerservaring onacceptabel wordt, creëer je een single point of failure.

⁶¹ Het product wordt hier slechts kort aangehaald en niet in detail beschreven, omdat het buiten de scope van het project ligt. Het scenario wordt hier als mogelijkheid naar voren gebracht omdat de use case waarin hij ingezet kan worden (ook hier beschreven) zich in de toekomst voor zou kunnen doen.

Wanneer in te zetten:

Bij erg grote klanten. Als de kinderwerkplek op een grote basisschool ingezet wordt, waar wellicht tussen de 50 en 100 werkplekken tegelijkertijd multimedia content moeten afspelen, kan de 'branch repeater' veel breedte besparen (zo'n 25%⁶²).

4.2.4 Conclusie:

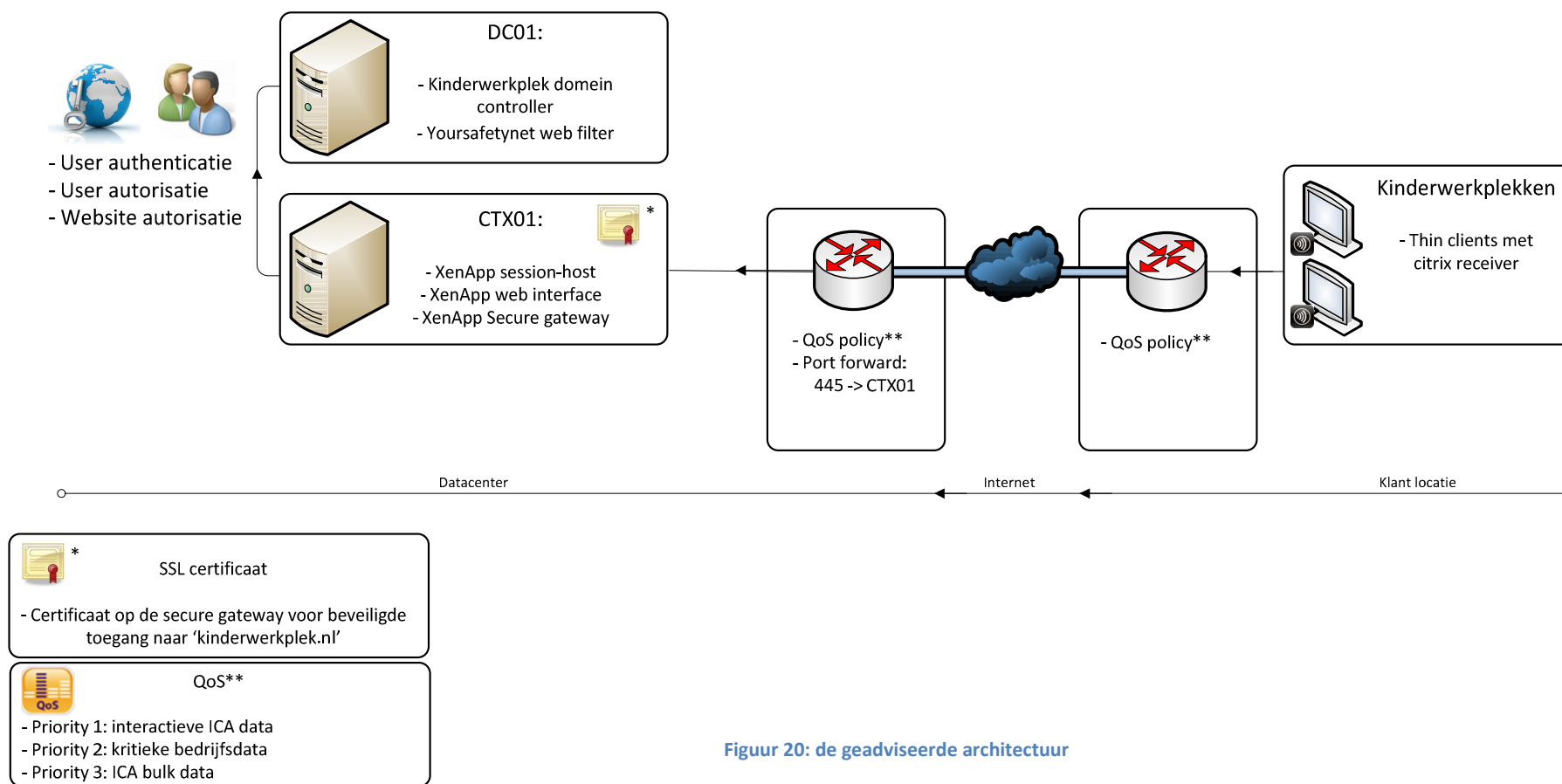
De tweede optie (web interfance) is de meest flexibele. Door gebruik te maken van Secure Gateway (Citrix) of Remote Gateway (RDS) kunnen de clients connectie maken met de Citrix receiver of RDP client respectievelijk. Daarnaast zullen de desktops en applicaties ook beschikbaar zijn vanaf de browser. Als er dan ooit besloten wordt om de kinderwerkplek aan te gaan bieden aan thuisgebruikers, is dat al mogelijk met deze oplossing.

Daarnaast is het dan niet nodig klanten op te nemen in de VPN, maar is het wel mogelijk als dit gewenst is.

⁶² Performance Assessment and Bandwidth Analysis for Delivering XenDesktop to Branch Offices (<http://support.citrix.com/servlet/KbServlet/download/23001-102-642442/XenDesktop%20to%20Branch%20Offices.pdf>)

4.3 Het advies (conclusie):

Hiervoor is geconcludeerd dat XenApp het beste pakket is, en dat deze het beste ingezet kan worden met de 'secure gateway'. XenApp is beter schaalbaar en zal responsiever blijven onder suboptimale omstandigheden; de 'secure gateway' geeft een flexibele manier om desktops aan te bieden via XenApp. Deze oplossing ziet er als volgt uit:



Figuur 20: de geadviseerde architectuur

Bronvermeldingen:

Algemeen gebruikte bronnen:

Hieronder de bronnen die regelmatig geraadpleegd zijn tijdens het project:

Websites:

<http://support.citrix.com/>

<http://technet.microsoft.com/nl-nl/ms376608.aspx>

<http://www.brianmadden.com/>

Specifieke bronnen gebruikt in dit document:

Deze bronnen zijn gebruikt en vermeldt in dit document. Hier worden ze nog eens allemaal op een rij gezet:

Kinderwerkplek website:

<http://www.kinderwerkplek.nl/index.php/component/content/?view=featured&Itemid=101>

Definitie protocol:

<http://www.vandale.nl/opzoeken?pattern=protocol&lang=nn>

De gemiddelde snelheid van internetconnecties in nederland:

<http://www.akamai.com/stateoftheinternet/>

RDS QoS:

<http://social.technet.microsoft.com/Forums/da-DK/winserverTS/thread/ee61ee0c-2ea6-4cac-8eee-e7fc268d490d>

RemoteFX:

<http://blogs.msdn.com/b/rds/archive/2012/06/13/remote-desktop-services-what-s-new-in-windows-server-2012-release-candidate.aspx>

Microsoft RemoteFX for Virtual Desktop Infrastructure: Architectural Overview [abstract]

(<http://www.microsoft.com/en-us/download/details.aspx?id=13864>)

RemoteFX for WAN:

<http://blogs.msdn.com/b/rds/archive/2012/08/23/remotefx-for-wan-overview-of-intelligent-and-adaptive-transports-in-windows-8-and-windows-server-2012.aspx>

TCP:

<http://www.tebyan.net/newindex.aspx?pid=31159&BookID=23760&PageIndex=158&Language=3>

RemoteFX:

<http://blogs.msdn.com/b/rds/archive/2012/08/16/enabling-a-seamless-multimedia-experience-with-remotefx-media-streaming-in-windows-server-2012-and-windows-8.aspx>

ICA virtual channels:

<http://ctxvm.blogspot.nl/2011/07/ica-virtual-channels.html>

Packet tagging:

http://support.citrix.com/servlet/KbServlet/download/23-102-665062/ICA_Priority_Packet_Tagging_FINAL.pdf

What do we mean by enhanced QoS?

<http://blogs.citrix.com/2011/08/25/enhanced-qos-via-multi-stream-ica/>

Adaptive display:

<http://bramwolfs.com/2012/05/08/adaptive-display-whats-in-the-game-and-do-we-need-to-fine-tune/>

XenApp flash tests:

<http://www.vmware.com/files/pdf/techpaper/PCoIPvHDXsinglesession03-05-12.pdf>

Codecs:

<http://support.citrix.com/article/CTX104912>

HDX:

<http://support.citrix.com/servlet/KbServlet/download/29626-102-684449/HDX%20Optimization%20and%20Best%20Practices.pdf>

Websense:

<http://www.websense.com/content/TRITON-solutions.aspx>

Span poort:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml

Websense architectuur:

<http://www.websense.com/support/article/t-kbarticle/Network-Agent-configuration-and-setup>

Hyper-V SPAN:

http://technet.microsoft.com/en-us/library/jj679878.aspx#bkmk_portmirror

Yoursafetynet:

<http://www.yoursafetynet.com/page/over-ons/over-yoursafetynet/onzehistorie/>

Yoursafetynet manual:

<https://www.yoursafetynet.com/files/modules/content/uploads/downloads/support/yoursafetynet-school-gebruikershandleiding-nl.pdf>

Worker groups:

<http://support.citrix.com/proddocs/topic/xenapp6-w2k8-admin/ps-maintain-worker-groups.html>

Performance Assessment and Bandwidth Analysis for Delivering XenDesktop to Branch Offices

(<http://support.citrix.com/servlet/KbServlet/download/23001-102-642442/XenDesktop%20to%20Branch%20Offices.pdf>)

Bijlage 1: Plan van aanpak:

Voorwoord:

In dit plan van aanpak worden de activiteiten van de komende maanden m.b.t. mijn afstudeeropdracht beschreven en gepland. Dit document vormt een dynamisch contract tussen de afstudeerder, Kinderwerkplek en de Hogeschool Utrecht. Zodra het document door alle partijen is goedgekeurd kan worden begonnen met de opdracht. Door nieuwe bevindingen kan het voorkomen dat de planning, werkwijze, of opdracht zelf aangepast moet worden; op dat moment zal het plan van aanpak aangepast worden en opnieuw ter goedkeuring worden opgeleverd.

Het document is stapsgewijs opgebouwd: eerst wordt het bedrijf beschreven en waar het naar toe wil (1), vervolgens welke problemen zich daarbij voordoen en welke dit project daarvan moet op moet gaan lossen (2), hier wordt de opdracht uit afgeleid en tot slot concreet gedefinieerd (3); de mijlpaalproducten die hierbij gemaakt worden staat in (4); in (5) wordt beschreven hoe wanneer ze tot stand komen; tot slot komt in (6) de projectomgeving aan bod (de geïnvolveerde partijen en het communicatieplan).

Inhoudsopgave

1. Bedrijfsinfo:.....	61
1.1 Algemene bedrijfs- en product informatie:.....	61
1.2 Organogram:	62
2. Probleemstelling:	63
2.1 Probleemstelling:.....	63
2.2.1 Gebruikersperspectief	63
2.1.2 Beheersperspectief:.....	64
2.2 Doelstelling:.....	64
2.2.3 Doelstelling:	64
2.2.1 Doelstelling in één kernzin :	Fout! Bladwijzer niet gedefinieerd.
3. Opdrachtsomschrijving:	68
3.1 Huidige situatie (RDS):	65
3.1.1 Conceptuele weergave.....	65
3.1.1 Technische omgeving	65
3.2 Gewenste situatie:	68
3.2.1. Gebruikerseisen:	68
3.2.2 Beheerseisen:.....	69
3.3 De opdracht:.....	70
3.3.1 Structuur adviesrapport:.....	70
3.3.2 Client side:	71
3.3.3 Protocol:.....	71
3.3.4 Pakket:.....	72
3.4 Projectgrenzen:	73
3.4.1 Scope:.....	73
3.4.2 Tijd:.....	74
3.4.3 Budget:	74
3.4.4 kwaliteit:	74
4. Mijlpaal producten:.....	75
4.1 Plan van aanpak:.....	75

4.2 Productvergelijkingsmatrix:.....	75
4.3 Adviesrapport:	75
4.4 Proof of concepts:.....	75
4.5 Scriptie:	75
5. Methode:.....	76
5.1 Pakketselectie:	76
5.2 Onderzoek:.....	77
6. Planning:.....	78
6.1 Fasering en aanpak:.....	78
6.1.1. Oriëntatie:	78
6.1.2 Hoofdfase (adviesrapport / scriptie):.....	79
6.1.3 Afronding:.....	80
6.2 Planning:	81
6.2.1 Tabel:.....	81
6.2.2 Gantt chart:	83
7. Projectomgeving:	84
7.1 Partijen:	84

1. Bedrijfsinfo:

1.1 Algemene bedrijfs- en product informatie:

Het bedrijf Kinderwerkplek, opgericht door Marco van Thiel, levert zogenaamde ‘kinderwerkplekken’⁶³ aan basisscholen, buitenschoolse opvang en kinderdagverblijven. De kinderkwerplek is een computer geïntegreerd in een meubel die enerzijds kinderen een veilige en educatieve computeromgeving biedt en anderzijds gebruikersgemak en minimaal onderhoud voor het personeel van de scholen.

Het idee is dat de kinderen veilig kunnen internetten en educatieve software kunnen gebruiken zonder dat de leraren daar moeite voor hoeven te doen (d.w.z. plug-and-play in de meest strikte zin van het woord). Om dit te bewerkstelligen wordt er gebruik gemaakt van ‘thin clients’ die verbinding maken met de servers van Kinderwerkplek om de kinderen een desktop aan te bieden.

Op de site⁶⁴ wordt het product als volgt beschreven:

“Heeft u een buitenschoolse opvang, kinderdagverblijf of bent u directeur van een basisschool? Bent u op zoek naar een mogelijkheid om uw kinderen op een veilige en educatieve manier gebruik te laten maken van computers en internet? Ziet u op tegen alle technische vragen die dat gaat opleveren? Heeft u ook last van computers die het regelmatig niet doen, of dat er weer een of andere update geïnstalleerd moet worden? Dan bieden wij -de perfecte oplossing voor u:

De Kinderwerkplek is een kleurige computerlessenaar voor vier kinderen waarin de computers veilig weggewerkt zijn. De bijgeleverde computers worden door ons geïnstalleerd met educatieve software en een sterke internetfilter. Daarnaast leveren we standaard een doorlopend servicecontract voor het ICT beheer. Hebt u extra wensen? Dan bieden wij speciaal voor u op maat gemaakte uitbreidingsopties.

U en uw medewerkers hoeven zich nooit meer druk te maken over de hard- en de software, alles is geregeld. Het enige wat u hoeft te doen, is de kinderkwerplek aan- en uit te zetten.”

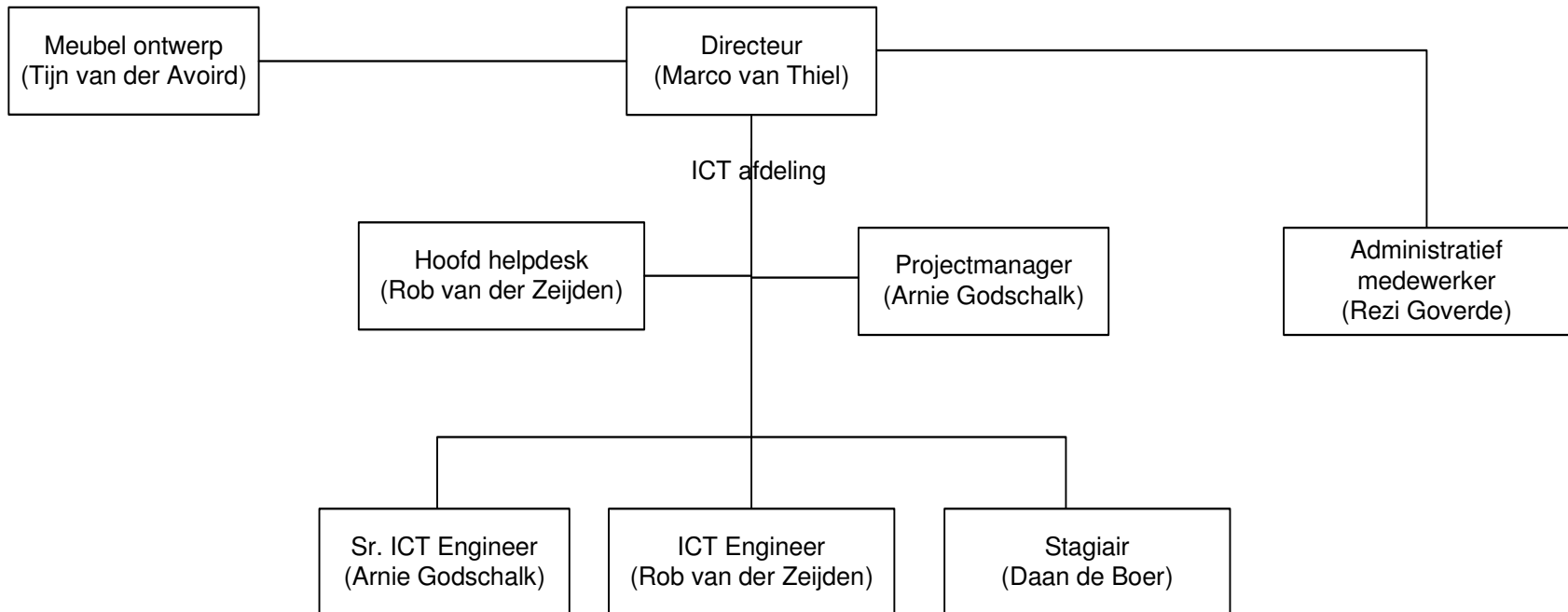
⁶³ Omdat het bedrijf en product dezelfde naam hebben, zal ik in het gehele document aan het bedrijf refereren met een hoofdletter (Kinderwerkplek) en aan het product zonder hoofdletter (kinderwerkplek), om eventuele verwarring te voorkomen.

⁶⁴ <http://www.kinderwerkplek.nl/index.php/component/content/?view=featured&Itemid=101>

1.2 Organogram:

Tipdesign B.V. (partner)

ICT plek B.V.



2. Probleemstelling:

2.1 Probleemstelling:

2.2.1 Gebruikersperspectief

De kinderwerkplek is een 'thin client' geïntegreerd in een meubel. Deze client maakt een RDP verbinding met 'Remote desktop services' (voortaan RDS) in een datacenter; de gebruiker krijgt vervolgens van RDS een desktop aangeboden. Deze opzet werkt in grote lijnen en heeft al enkele malen proef gedraaid⁶⁵.

Toch wordt er aan een aantal essentiële eisen niet voldaan. Dit is gebleken uit interviews met de doelgroep, de kinderen. Hieronder een citaat uit een interview met een groep demo gebruikers:

"De kinderen waren niet tevreden over de snelheid van het internet, het laden van pagina's duurde erg lang en resulteerde soms zelfs in het vastlopen van de computer. Ook vonden de kinderen dat er teveel [internet toegang] afgeschermd werd. [...] Ze gaven aan dat bijvoorbeeld informatie over boeken van Carry Slee die over drugs en geweld gaan ook allemaal afgeschermd werden. De kinderen vonden dat er pakketten voor onderbouw en bovenbouw zouden moeten zijn. Hierdoor is er voor elke leeftijd wat wils."⁶⁶

De aangeboden desktops zijn niet responsief genoeg tijdens het afspelen van (flash) filmpjes; daarnaast heeft de webfilter nog niet de juiste balans tussen veiligheid en toegankelijkheid. Tot slot moet er content te vinden zijn voor de verschillende groepen kinderen.

⁶⁵ Op het moment staat er een demo in het 'Tilburg innovation center' (<http://www.t-ic.nl/>).

⁶⁶ ICT Werkplek B.V.: Operationeel marketingplan; Pieter Kellendonk (2012)

2.1.2 Beheerspectief:

Op het moment draait er enkel een demo van de kinderwerkplek; de verwachting is echter dat er binnen een jaar steeds meer kinderwerkplekken uitgerold gaan worden. Door het verbeteren van de techniek en de meubel kan de kinderwerkplek hernieuwd aangeboden worden aan de klant; hierbij zal vooral de zomervakantie periode belangrijk zijn, dit is doorgaans bij scholen de periode waar budgetbeslissingen gemaakt worden m.b.t. ICT.

De huidige opstelling kan nog niet aan alle eisen voldoen (vgl. 2.1.1) en als het aantal werkplekken zoals verwacht gaat groeien zal de performance enkel verslechteren.

Er moet derhalve gezocht worden naar een oplossing die aan de eisen voldoet, maar die ook schaalbaar is. 'Schaalbaarheid' is in verschillende problemen te analyseren:

- Bij groei van de kinderwerkplek zal de infrastructuur in het datacenter van het bedrijf (regelmatig) uitgebreid moeten worden;
- Bij uitbreiding van het aantal werkplekken op één locatie zal de internetverbinding steeds voller raken, waardoor er minder bandbreedte per desktop beschikbaar is en de responsiviteit kan afnemen; het protocol moet hier rekening mee kunnen houden en zich aan kunnen passen;
- Het applicatieaanbod zal met het aantal klanten groeien; het kan dan lastig worden om te blijven overzien welke applicaties er draaien en wie ze aangeboden krijgt; het gebruikte pakket moet het mogelijk maken pakketten logisch te organiseren.

Daarnaast is de huidige situatie nog niet voldoende gedocumenteerd. Dit is—zowel voor de huidige-als toekomstige situatie— wel wenselijk.

2.2 Doelstelling:

2.2.3 Doelstelling:

De doelstelling is om een advies te leveren m.b.t. een schaalbare infrastructuur die kinderwerkplekken aan kan bieden met hoge kwaliteit multimedia. Dit advies moet gedurende verschillende groeistadia van de kinderwerkplek te gebruiken zijn. Dit betekent dat er in het advies verschillende oplossingen in verschillende prijsklassen naar voren moeten komen. *Met dit advies moet het bedrijf de infrastructuur op kunnen zetten en pakketselectie kunnen uitvoeren.*

Het advies moet het bedrijf op twee manieren helpen:

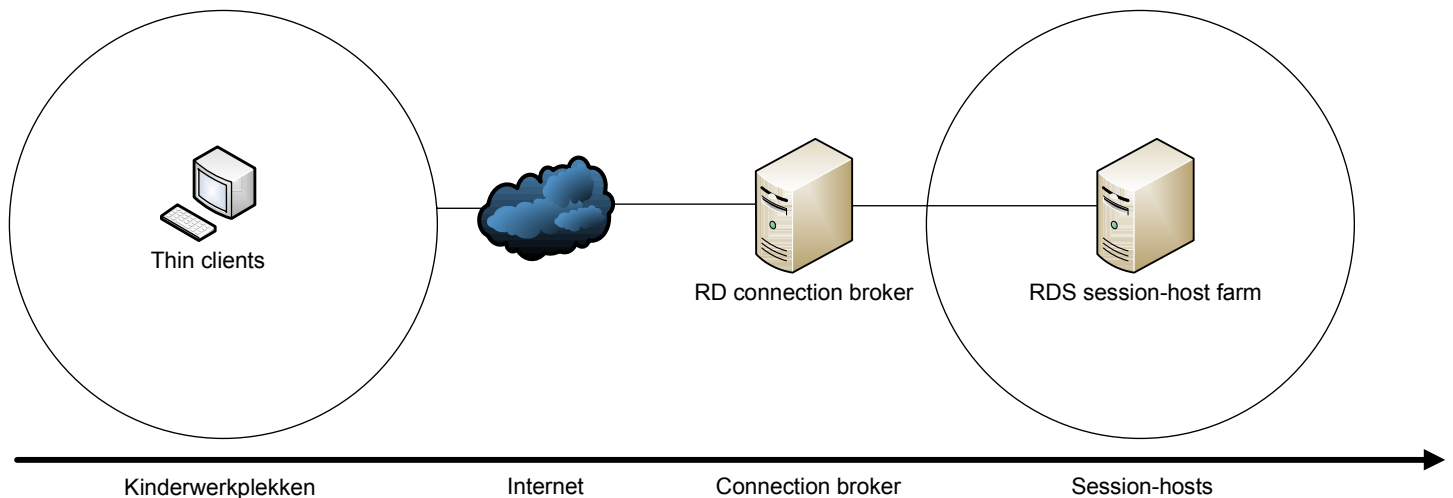
- Door het verbeteren van de gebruikerservaring de aantrekkelijkheid van het product vergroten, en zodat er meer kinderwerkplekken verkocht kunnen worden;
- Zorgen voor een schaalbare infrastructuur zodat er zonder zorgen kinderwerkplekken uitgerold kunnen worden, zonder dat de performance achteruit gaat.

2.3 Huidige situatie (RDS):

Hier wordt de probleemstelling in meer technisch-detail beschreven, d.m.v. een analyse van de huidige situatie. In het volgende hoofdstuk kan dan door de huidige situatie met de gewenste- te vergelijken de opdracht uiteengezet worden.

2.3.1 Conceptuele weergave

De huidige situatie is hieronder conceptueel weergegeven:



De thin clients laden een klein OS (Windows 7 embedded) waarop een RDP client draait. Deze connect met de RDS connection broker in het data center bij Routelt; dit is een server die onder andere de inkomende RDP connecties verdeelt tussen de 'RD session hosts' in de farm. De verbinding makende thin client wordt toegewezen aan een 'session host' en krijgt een desktop te zien.

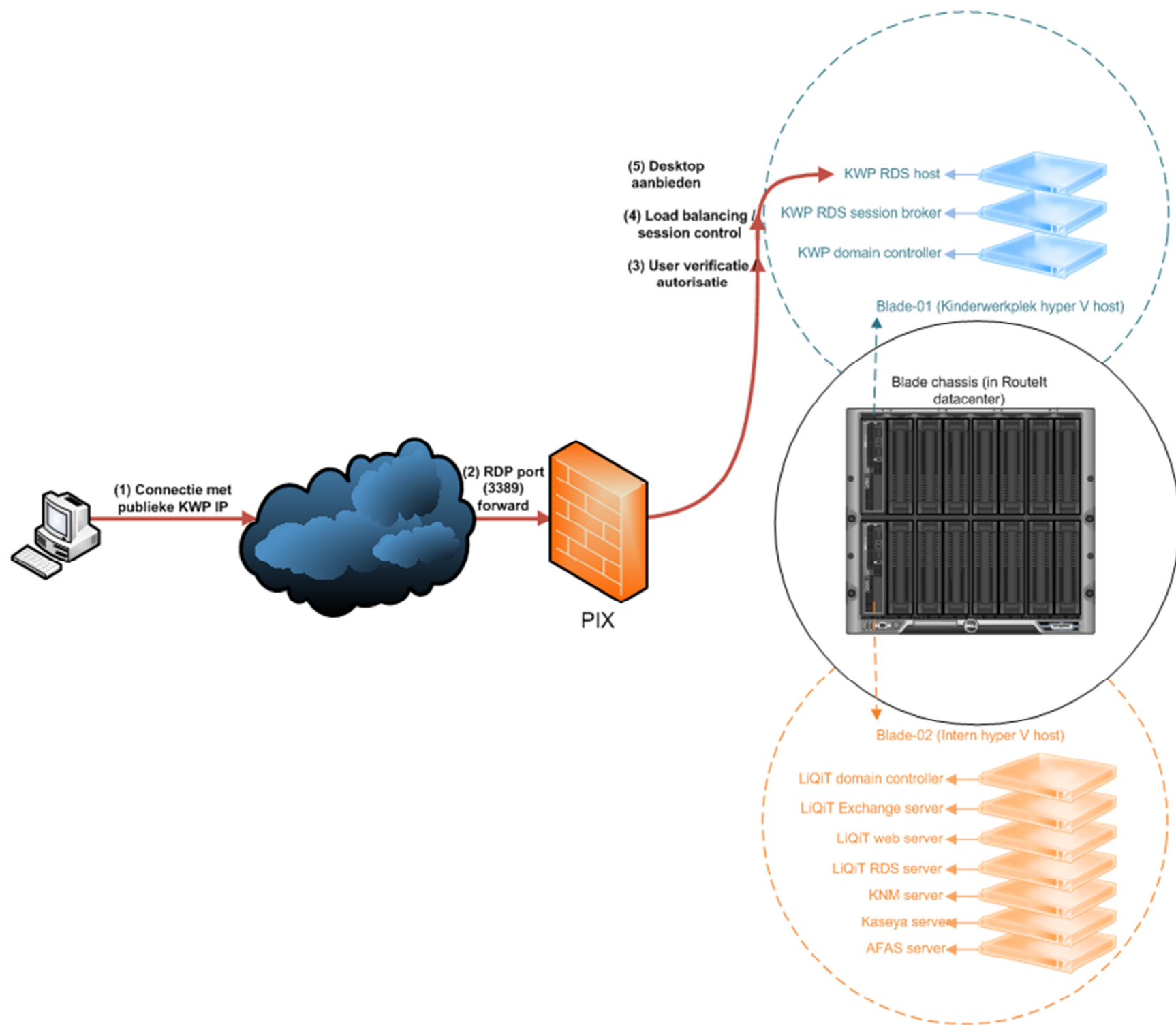
Op deze desktop zijn (educatieve) spelletjes te vinden en kan gebruik gemaakt worden van internet. De gebruiker wordt d.m.v. policies beperkt tot het gebruiken van geautoriseerde programma's en Windows functies.

2.3.2 Technische omgeving

De servers zijn virtuele machines op Hyper-V hosts (blades in het Routelt data center). Er zijn in totaal twee blades: één voor LiQiT (intern) en één voor Kinderwerkplek.

Hieronder een tekening die de Hyper-V hosts en de daarop staande virtuele servers laat zien, alsmede de weg die een client aflegt naar zijn virtuele desktop⁶⁷:

⁶⁷ De stappen zijn genummerd en worden onder de tekening verder toegelicht.



1. De thin clients starten een klein image (Windows Embedded) die automatisch een RDP verbinding maakt met het publieke IP van de kinderwerkplek
2. Op de firewall staat een port forward die zorgt dat de aanvraag van de client op de session broker terecht komt.
3. Eenmaal intern worden eerst de credentials van de user gecontroleerd
4. De session broker houdt de load op de servers bij en de lopende sessies van de gebruikers. Op basis van load balancing policies wordt beslist op welke host de sessie gaat draaien en hoeveel resources hij mag verbruiken;
5. De gebruiker krijgt van de gekozen host een desktop sessie.

3. Opdrachtomschrijving:

3.1 Gewenste situatie:

De gewenste situatie komt in grote lijnen overeen met de huidige situatie, de architectuur blijft gelijk: een client maakt connectie met een session broker, die een desktop verschaft. De huidige omgeving moet echter zodanig opnieuw worden ingericht, dat aan de verschillende eisen (gedeeltelijk impliciet beschreven in **2.1 probleemstelling**) voldaan wordt. Om deze eisen concreter in kaart te brengen worden ze hieronder geëxpliciteerd. Vervolgens wordt in de volgende paragraaf een tentatieve lijst met oplossingen gegeven die aan deze eisen kunnen voldoen, en daarom de komende periode onderzocht zullen worden.

Uit de probleemstelling (2.1) kunnen technische eisen afgeleid worden waaraan op dit moment niet voldaan wordt. Deze worden ingedeeld onder eisen m.b.t. de gebruiker en m.b.t. beheer, conform deze paragraaf (probleemstelling). Dit gebeurt in 3.2.1 en 3.2.2. Vervolgens wordt de opdracht van het project als zodanig uiteengezet in 2.2.3 (d.w.z. wat ik ga doen om het bedrijf in staat te stellen aan de genoemde eisen te voldoen).

3.1.1. Gebruikerseisen:

Functionele eisen:

- Het internetfilter moet flexibel zijn:
 - Afhankelijk van de groep en/of leeftijd van het kind moeten verschillende onderwerpen gefilterd worden, zodat de internetfilter een balans vindt tussen veiligheid en toegankelijkheid;
 - Het zou desastreus voor het product zijn als de kinderwerkplek gelijk gebruikt zou worden om sites te bezoeken die niet voor kinderen bedoeld zijn (en als dit niet beveiligd wordt, gebeurt dit ook). Daarom worden initieel alle traditionele onderwerpen geblokkeerd: drugs, wapens, gokken, porno, naakt. Vervolgens wordt in overleg met de begeleiders en kinderen de filter waar nodig toegankelijker gemaakt. Het is beter eerst te veilig te zijn en dan naar onder aan te passen dan andersom (vgl. volgende punt).
 - Op aanvraag moeten bepaalde (combinaties van) onderwerpen of specifieke sites toegelaten worden (i.c. Carry Slee + drugs) d.m.v. whitelisting.
- Er moeten pakketten voor zowel onder- als bovenbouw beschikbaar zijn; idealiter worden afhankelijk van de groep van het kind specifieke pakketten aangeboden d.m.v. (AD geïntegreerde) gebruikersgroepen die aan bepaalde pakketten gekoppeld kunnen worden.

Technische eisen:

- De externe desktop moet responsief blijven, zelfs bij suboptimale internet verbindingen (zoals dikwijls het geval is bij b.v. basisscholen);
 - o 'responsief' is hier ambigu, een objectieve schaal voor acceptabele responsiviteit is naar mijn weten (en na enig onderzoek) nog niet gemaakt. Ik heb enkel anekdotisch bewijs (uit eigen ervaring) dat 0-150 milliseconde vertraging het gevoel van een fysieke desktop geeft; 150-300 ms acceptabel is en hoogstens kleine frustraties oplevert (het voelt enigszins traag, maar het is niet te zien), en alles boven 300ms vervelend is om mee te werken. Overigens is er wel onderzoek gedaan naar de mate waarin video en audio asynchroon kunnen lopen, voordat het onacceptabel wordt voor de gemiddelde mens; mocht een bepaald pakket of protocol, door prioriteiten te stellen tussen video en audio, asynchroniteit introduceren tussen de twee, moet deze tussen de 22ms blijven⁶⁸. *Initieel zal er gewerkt worden met een acceptatiegrens van maximaal 300ms op responsiviteit (maar idealiter blijft hij onder 150ms).*

3.1.2 Beheerseisen:

De oplossing moet zowel inhoudelijk als resource-technisch schaalbaar zijn

Functionele eisen:

- 'On the fly' toevoegen van nieuwe applicaties
- Toevoegen van gebruikersgroepen met eigen aangepaste webfilter en applicatieaanbod

Technische eisen:

- Uitbreiden van storage zonder onderliggende architectuur aan te passen
- Uitbreiden van server farm zonder onderliggende architectuur aan te passen
- Intelligent kunnen verdelen van serverload d.m.v. load balancing policies

3.1.3 Analyse van de eisen:

In 3.1.1 en 3.1.2 werd een eerste karakterisering van de eisen gegeven; deze kunnen verder gepreciseerd worden aan de hand van de 'James McCabe' methode; dit wordt in bijlage 1 gedaan.

⁶⁸ Sara Kudrle et. al. (July 2011). "Fingerprinting for Solving A/V Synchronization Issues within Broadcast Environments". Motion Imaging Journal (SMPTE). "Appropriate [audio]/[video] sync limits have been established and the range that is considered acceptable for film is +/- 22 ms. The range for video, according to the ATSC, is up to 15 ms lead time and about 45 ms lag time"

3.2 De opdracht:

De opdracht is om een adviesrapport uit te brengen die beschrijft hoe de gewenste situatie bereikt kan worden. Dit wordt gedaan door verschillende oplossingen te onderzoeken die aan bovenstaande eisen voldoen en vervolgens een adviesrapport uit te brengen met de bevindingen van het onderzoek. Deze moet de prijs / kwaliteit verhoudingen van de pakketten in kaart brengen, zodat het bedrijf hierop terug kan vallen gedurende verschillende groeistadia van de kinderwerkplek.

In dit hoofdstuk wordt eerst de structuur van dit adviesrapport besproken (3.3.1) en vervolgens de drie onderzoeksgebieden van mogelijke oplossingen (client-side, protocol en pakket, 3.3.2 t/m 3.3.4 respectievelijk).

3.2.1 Structuur adviesrapport:

In **2.2.3 doelstelling** kwam de structuur van het adviesrapport al naar voren: er moet niet alleen een ideale oplossing beschreven worden, maar verschillende oplossingen voor verschillende prijzen, die Kinderwerkplek op een flexibele manier kunnen ondersteunen. Hieronder wordt de structuur uiteengezet die dit moet realiseren:

- Beschrijving ideale oplossing
 - Introductie / achtergrond oplossing
 - Mogelijkheden en voordelen (gebaseerd op bovenstaande technische eisen)
 - Relevantie voor de kinderwerkplek
 - Kosten
- Beschrijving alternatieve oplossingen
 - Introductie / achtergrond oplossing
 - Mogelijkheden en voordelen (gebaseerd op bovenstaande technische eisen)
 - Relevantie voor de kinderwerkplek
 - Kosten
- Vergelijkingsmatrix met kosten en mogelijkheden tussen verschillende oplossingen⁶⁹
- Implementatieplannen voor de oplossingen die levensvatbaar zijn bevonden
 - Vereisten
 - Voorbereiding implementatie
 - Technische handleidingen m.b.t. pakket implementatie
 - Onderhoud
 - Lopend onderhoud
 - Uitbreiding aanbod
 - Uitbreiding resources
 - Hoe kan de oplossing aangeboden / ingezet worden

⁶⁹ Deze zal op een later tijdstip geleverd worden; na het inleveren van de scriptie wordt een testoplossing gebouwd op de werkelijke kinderwerkplek servers; deze oplossing wordt op een beurs tentoongesteld. Als dit allemaal goed gaat, schrijf ik een implementatieplan op basis van deze opstelling.

- Vergelijkende proof of concepts

Dit adviesrapport moet natuurlijk gevuld worden met (nog te onderzoeken) oplossingen. Hiervan kan alvast een provisionele lijst worden gemaakt. Uit de huidige- en gewenste situatie kwamen de te onderzoeken oplossingen namelijk al naar voren: om de gebruikerservaring te verbeteren zijn er slechts drie mogelijke opties:

- Aan de client side (thin / zero clients)
- D.m.v. een ander protocol
- D.m.v. een pakket dat beter gebruik weet te maken van het huidige protocol (RDP)

De enige andere mogelijkheid is een snellere internetverbinding te gebruiken, maar dit is niet iets waar het bedrijf over beslist, het is de internetverbinding van de klant. De oplossing moet op een acceptabel niveau blijven functioneren zelfs bij minder snelle verbindingen.

Deze drie onderdelen zullen worden onderzocht en verwerkt in het adviesrapport:

3.2.2 Client side:

Het concept van thin clients is dat er zo min mogelijk aan de client side gebeurt. Dit betekent dat bijvoorbeeld media door de server gedecodeerd wordt en volledig over lijn wordt gestuurd.

Er kan gekeken worden naar thin- of zero clients die een ingebouwde videokaart of media decoder hebben. De media kan dan gecodeerd (en dus kleiner) over de lijn gestuurd worden. Er moet uitgezocht worden hoeveel extra kosten dit met zich meebrengt en of dit levensvatbaar is voor de kinderwerkplek.

3.2.3 Protocol:

De huidige oplossing gebruikt RDP en voldoet niet aan de eisen. Uit het onderzoek moet blijken of de huidige problemen intrinsiek zijn aan het RDP protocol of veroorzaakt worden door het gebruikte pakket of implementatie.

Het met RDP concurrerende protocol is ICA. In het onderzoek moeten de relevante verschillen tussen de twee naar voor komen. Er moet beschreven worden wat de voor- en nadelen van de twee zijn en welke beter past bij de kinderwerkplek.

3.2.4 Pakket:

In het afstudeervoorstel zijn reeds een aantal pakketten benoemd die onderzocht moeten worden. Ze worden onderzocht aan de hand van de genoemde eisen. Gemakshalve wordt daar hieronder een overzicht van gegeven (enkel de eisen relevant aan pakketselectie):

Functioneel:

- 'On the fly' toevoegen van pakketten
- Mogelijkheid voor gebruikersgroepen met aangepaste webfilter en applicatieaanbod

Technisch:

- De vertraging in de verbinding met de virtuele desktop mag niet boven 300ms komen;
- Video en audio mogen niet meer dan 22ms asynchroon lopen;
- Uitbreiden van server farm zonder architectuur aan te passen
- Intelligent verdelen van server load d.m.v. load balancing policies

De volgende pakketten worden onderzocht; ze zijn gekozen omdat ze vanuit het bedrijf uit genoemd zijn en de meest gebruikte pakketten in hun respectievelijke prijsklasse zijn ⁷⁰:

- **Remote desktop services (RDS):**

RDS wordt momenteel al gebruikt in de testopstelling van de kinderwerkplek. Deze kan echter niet goed genoeg overweg met multimedia. Microsoft heeft echter kort geleden een nieuwe techniek uitgebracht genaamd 'RemoteFX'. Deze moet hoge kwaliteit multimedia kunnen faciliteren. Dit moet onderzocht en getest worden, uiteindelijk in een vergelijkend proof of concept met de andere oplossingen. Omdat RDS geleverd wordt met Windows 2008 (die al gebruikt wordt) is het enkel nodig CAL's aan te schaffen, waardoor deze oplossing relatief goedkoop zal zijn.

- **Citrix Xenapp:**

Xenapp levert virtuele desktops en applicaties aan gebruikers, net zoals RDS. Citrix hanteert echter een gesofisticeerder protocol dan RDP (genaamd ICA) en staat bekend om zijn goede multimedia ondersteuning met de 'HDX' techniek. Voor Xenapp zal het echter nodig zijn zowel CAL's als Citrix licenties aan te schaffen, wat de oplossing duur maakt.

- **2X (Vervallen):**

Er is besloten dit pakket niet mee te nemen in het onderzoek. Er is gebleken dat RDS en Citrix samen al een groot deel van het prijs / kwaliteits spectrum vullen. Daarnaast moet je voor 2X niet alleen 2X licenties hebben, maar ook RDS licenties. Als je Citrix gebruikt moet je zelfs 2X, RDS én Citrix licenties gebruiken. De kosten lopen dan al snel uit de hand.

⁷⁰ In volgorde van goedkoper naar duurder: RDS, 2X, Xenapp.

Daarnaast is het niet duidelijk wat 2X voor meerwaarde kan leveren op het gebied van multimedia. Meerdere pogingen (6 om precies te zijn) om contact op te nemen met het sales team hebben niets opgeleverd. Ook posts op de officiële forums hielpen niet. De kosten, samen met de slechte eerste indruk van de ondersteuning van dit product, hebben het besluit geforceerd dit pakket niet mee te nemen.

3.3 Projectgrenzen:

3.3.1 Scope:

Binnen de grenzen van het project valt het opleveren van een adviesrapport waarin beschreven wordt in welke mate de onderzochte pakketten aan de eisen voldoen, en hoe ze in grote lijnen geïmplementeerd kunnen worden. Daarnaast vallen binnen de projectgrenzen een productvergelijkingsmatrix komen en vergelijkbare proof of concepts.

Een eventuele daadwerkelijke implementatie en concreet implementatieplan valt buiten het project⁷¹.

Hieronder een MoSCoW analyse om de afbakening te verhelderen:

- **Must have:**
 - Advies m.b.t. een schaalbare infrastructuur die kwaliteit multimedia ondersteund:
 - Advies over client-side oplossingen
 - Advies m.b.t. mogelijk te gebruiken protocollen
 - Advies over mogelijk te gebruiken pakketten
 - Vergelijkende proof of concepts
 - Prijs-kwaliteitsvergelijkingsmatrix tussen de verschillende oplossingen
 - Implementatieplannen voor de levensvatbare oplossingen
 - Technische implementatie (hoe kan deze oplossing opgezet worden)
 - Strategische implementatie (hoe kan deze oplossing ingezet worden)
- **Should have:**
 - Advies m.b.t. alternatieve mogelijkheden om de kinderwerkplek aan te bieden (op mobile devices bijvoorbeeld, of vanuit de cloud)
- **Could have:**
 - Advies m.b.t. het integreren van de 'Nova Touch' software⁷²
- **Won't have:**
 - Advies m.b.t. het aanbieden van complete virtuele machines aan gebruikers (dit is te duur en onnodig in deze use case)

⁷¹ Hoewel het buiten het project valt kan ik hier uiteraard wel aan meewerken tijdens de uitlooperperiode, mocht er besloten worden dit uit te voeren.

⁷² Er is als tip vanuit het bedrijf meegegeven dat het meeleveren van 'Nova Touch' software op de virtuele desktops het mogelijk kan maken op de kinderwerkplekken touch screens te gaan gebruiken; de prioriteit is natuurlijk om eerst de kinderwerkplek überhaupt te ronden, vandaar dat deze onder 'Could have' staat.

3.3.2 Tijd:

De opdracht als zodanig loopt van 1-10-12 tot en met 23-12-12. Daarvoor is een korte periode oriëntatie (Plan van aanpak periode) en daarna een periode om werkzaamheden op het bedrijf af te ronden (vgl. fases en planning in het volgende hoofdstuk).

3.3.3 Budget:

Er is geen budget opgesteld voor de opdracht. De reden hiervoor is dat er verschillende oplossingen geadviseerd worden tegen verschillende prijzen. De ideale oplossing kan op het moment te duur zijn, maar dat betekent niet dat hij buiten de grenzen van het project valt, omdat de doelstelling expliciet stelt dat het advies rekening moet houden met verschillende groeistadia van de kinderwerkplek.

3.3.4 kwaliteit:

De kwaliteit wordt vastgesteld d.m.v. de opgestelde eisen. De ideale situatie die wordt beschreven in het adviesrapport *moet* voldoen aan deze eisen. De ideale situatie fungeert namelijk als standaard waaraan de anderen oplossingen hun relatieve kwaliteit ontleen. Eventuele kwaliteiten die buiten de beschreven eisen vallen, staan buiten de scope van dit project, en worden niet meegenomen in het advies (omdat ze niet relevant zijn voor Kinderwerkplek, anders was het een eis geweest).

Ook voor de kwaliteitseisen kan een MoSCoW analyse verhelderend zijn:

- **Must have:**
 - Minder dan 300ms vertraging op de desktops;
 - Video en audio mogen niet meer dan 22ms asynchroon lopen;
 - Uitbreiden van server farm zonder architectuur aan te passen
 - Intelligent verdelen van server load d.m.v. load balancing policies
 - Uitbreiden van storage zonder onderliggende architectuur aan te passen
- **Should have:**
 - Minder dan 150ms vertraging
 - 'On the fly' toevoegen van pakketten
 - Mogelijkheid voor gebruikersgroepen met aangepaste webfilter en applicatieaanbod
 - Op aanvraag moeten bepaalde (combinaties van) onderwerpen of specifieke sites toegelaten worden (i.c. Carry Slee + drugs) d.m.v. whitelisting
- **Could have:**
 - AD integratie voor het verzorgen van groep specifieke content en filter
- **Won't have:**

4. Mijlpaal producten:

In dit hoofdstuk worden de mijlpaalproducten beschreven die opgeleverd moeten worden. Het betreft de volgende producten: 4.1: plan van aanpak; 4.2 productvergelijkingsmatrix; 4.3 adviesrapport; 4.4 proof of concepts en 4.5 scriptie.

4.1 Plan van aanpak:

Het document dat beschrijft hoe de rest van het onderzoek ingevuld zal worden en wat de opdracht precies inhoudt. Dit document kan gaandeweg aangepast worden indien nodig.

4.2 Productvergelijkingsmatrix:

Een belangrijk product dat deel uitmaakt van het adviesrapport. In deze matrix moet het bedrijf kunnen zien welke oplossing aan welke eisen voldoen en hoeveel ze kosten. Het bedrijf kan dan op verschillende momenten op basis van deze matrix beslissen welke oplossing het beste past bij de huidige situatie van de kinderwerkplek.

4.3 Adviesrapport:

Beschrijft de verschillende oplossingen in detail en benoemt de ideale oplossing. Daarnaast worden er implementatieplannen geleverd die laten zien hoe de oplossingen gebruikt en beheerd kunnen worden.

4.4 Proof of concepts:

Van elke oplossing die geschikt is bevonden voor de kinderwerkplek moet een proof of concept gemaakt worden. Deze kunnen dan onderling vergeleken worden om zo het bedrijf te ondersteunen in het maken van een beslissing.

4.5 Scriptie:

Alle bevindingen en gemaakte producten moeten worden beschreven in de scriptie die aan de HU opgeleverd zal worden. Hierin is te vinden wat het project inhield, hoe ik het precies uitgevoerd heb en wat de resultaten waren.

5. Methode:

5.1 Pakketselectie:

Op de HU hebben we een pakketselectie methode leren gebruiken die ook in dit project wordt toegepast. Deze methode voltrekt zich deels al in het plan van aanpak; de rest komt terug in het adviesrapport. Hieronder worden de stappen benoemd die de methode doorloopt⁷³:

1. Probleemstelling (PvA 2.1: probleemstelling)
2. Doelstelling: (PvA 2.2: doelstelling)
3. Opdrachtoomschrijving
 - a. Opstellen selectiecriteria (PvA 3.2: gewenste situatie)
 - b. Implementatieplan (PvA: 3.3.1 structuur adviesrapport)
 - c. Adviesrapport (PvA: 3.3.1 structuur adviesrapport)
4. Analyse van het probleem (PvA 3.1 huidige situatie)
5. Resultaten (gewenste situatie) (PvA 3.2: gewenste situatie)
6. Keuze pakketten en matrixtabel (AR: prijskwaliteitsproductvergelijkingsmatrix)
7. Implementatieplan (AR: implementatieplannen)
8. Conclusie en aanbeveling (AR: conclusie)

Het idee is dat de probleemstelling geformuleerd wordt en dat daaruit doelstelling voortkomt (nl. om het probleem op te lossen); hoe deze in algemene zin opgelost wordt vormt de opdrachtoomschrijving. Vervolgens wordt het probleem dieper geanalyseerd, waaruit dan concrete eisen (resultaten) komen. Deze worden gebruikt om pakketten aan te toetsen in een matrixtabel. Na de keuze wordt een implementatieplan gemaakt om deze keuze te implementeren. Dit wordt samengevat in een concrete conclusie en aanbeveling.

Dit is ook de structuur die in dit plan van aanpak (en dus gehele project) gehanteerd wordt.

⁷³ Per stap is, indien van toepassing, aangegeven waar in het PvA de stap is te vinden (bijvoorbeeld "PvA 2.1 probleemstelling"). Sommige stappen komen pas terug in het adviesrapport, deze worden aangegeven met 'AR' plus de naam van het hoofdstuk.

5.2 Onderzoek:

De methode van onderzoek verschilt naargelang het onderzochte onderwerp. De verschillende soorten onderwerpen worden ingedeeld in fases, om tijdens elke fase een eenduidige onderzoeksmethode aan te kunnen houden. Hoe dit precies ingedeeld wordt is in het volgende hoofdstuk te lezen.

Verder worden ter ondersteuning van het onderzoek de volgende methodes gebruikt:

5.2.1 MoSCoW:

MoSCoW wordt gebruikt om duidelijk te maken wat de prioriteit van elke eis is door ze te verdelen in: 'Must have', 'Should have', 'Could have' en 'Won't have'.

5.2.3 James McCabe:

Uit de 'James McCabe methode' wordt de 'analyse van de eisen' fase gebruikt. Dit omdat de eisen de kern van het project vormen. De eisen zijn natuurlijk in elk project van cruciaal belang, maar in dit project worden ze expliciet als beoordelingspunten gebruikt voor de pakketselectie (in de vergelijkingsmatrix); er kan dan beter een officiële methode gebruikt worden om de eisen zo precies mogelijk te maken.

In bijlage 1 staat deze analyse van de eisen. Hier wordt de informatie die reeds uit het plan van aanpak naar voren kwam (o.a. huidige situatie, eisen, enz.) kort en bondig volgens de McCabe methode uiteengezet, om als referentiepunt te dienen bij het adviseren van een oplossing in de volgende fase van het project.

Planning:

6.1 Fasering en aanpak:

Er zijn drie hoofdfases te onderscheiden in het project:

- Oriëntatie
- Adviesrapport / scriptie
- Afronding

Hieronder wordt beschreven hoe deze worden ingedeeld en aangepakt.

6.1.1. Oriëntatie:

Loopt van: 03-09-12 t/m 30-09-12.

De oriëntatiefase heeft de afgelopen weken plaatsgevonden. Tijdens deze periode is (grotendeels) ad-hoc onderzoek gedaan naar mogelijke vruchtbare onderzoeksonderwerpen die terug kunnen komen in het adviesrapport. Hierbij is vooral gebruikt gemaakt van de wensen van het bedrijf, dat voor de aanvang van de stage al een voorkeur had aangegeven.

De bedoeling was om een eerste indruk te krijgen van de verschillende onderwerpen en om te onderzoeken of de onderwerpen in ieder geval theoretisch toepasbaar zijn op de kinderwerkplek.

Het resultaat van de fase is dit document; dankzij het vooronderzoek kan hier beschreven worden wat er onderzocht gaat worden.

Deelproducten: plan van aanpak

6.1.2 Hoofdfase (adviesrapport / scriptie):

Loopt van: 01-10-12 t/m 23-12-12.

Deze fase vangt aan met de goedkeuring van het plan van aanpak en eindigt met het inleveren van de scriptie en het adviesrapport. Dit zijn de eindproducten van deze fase en het doel ervan.

Deze fase kan verder onderverdeeld worden:

- Onderzoek naar client-side oplossingen
- Onderzoek naar protocollen
 - o RDP
 - o ICA
- Onderzoek naar pakketten:
 - o RDS
 - o 2X
 - o XenApp
- Opzetten proof of concepts
- Samenbrengen bevinden in adviesrapport

Elk onderdeel wordt op verschillende wijze onderzocht:

- **Client-side oplossingen:**

Bij client-side oplossing wordt vooral gebruikt gemaakt internet om de specificaties en prijzen van de clients te vergelijken. Daarnaast wordt er op internet gezocht naar de verschillende wijzen waarop je deze clients in kan zetten. Het eindproduct, naast het adviesrapport, is een productvergelijking die de prijs en mogelijkheden van de verschillende clients naast elkaar zit. Dit wordt gepresenteerd aan het bedrijf, dat vervolgens kan beslissen of ze het in een proof of concept willen testen.

Deelproduct(en): Advies m.b.t. thin- en zero clients (mogelijkheden en functies), advies m.b.t. het inzetten van deze producten

- **Protocollen:**

Voor het protocollen onderzoek wordt gebruikt gemaakt van online documentatie en vakliteratuur. Zowel Citrix (ICA) als Microsoft (RDP) hebben een groot online documentatie archief waar deze informatie gevonden kan worden. Om nog dieper in te gaan op de details kan vakliteratuur gebruikt worden. Het doel is om uiteindelijk te kunnen beschrijven en onderbouwen welk protocol past bij de kinderwerkplek. Dit komt terug in het adviesrapport.

Deelproduct(en): Samenvatting werking RDP en ICA, beschrijving van relevante verschillen tussen de twee, onderbouwing van protocolkeuze voor kinderwerkplek.

- **Pakketten:**

Voor de pakketselectie wordt de documentatie gebruikt die bij het product geleverd wordt en indien nodig vakliteratuur. Daarnaast worden de pakketten getest en de ondervindingen bijgehouden. Hierbij wordt constant een oog gehouden op de eisen, zodat per pakket bekend is aan welke eisen wel en niet voldaan wordt. Deze informatie wordt gebruikt in de prijskwaliteitsvergelijkingsmatrix. Het doel is genoeg kennis op te doen over de pakketten om een advies te kunnen brengen aan het bedrijf en proof of concepts op te kunnen leveren.

Deelproduct(en): eisen-checklist per pakket, implementatiehandleidingen, prijsvergelijkingsmatrix.

6.1.3 Afronding:

Loopt van: 24-12-12 t/m 31-01-13.

Hier wordt eventuele lopende zaken binnen het bedrijf afgerond.

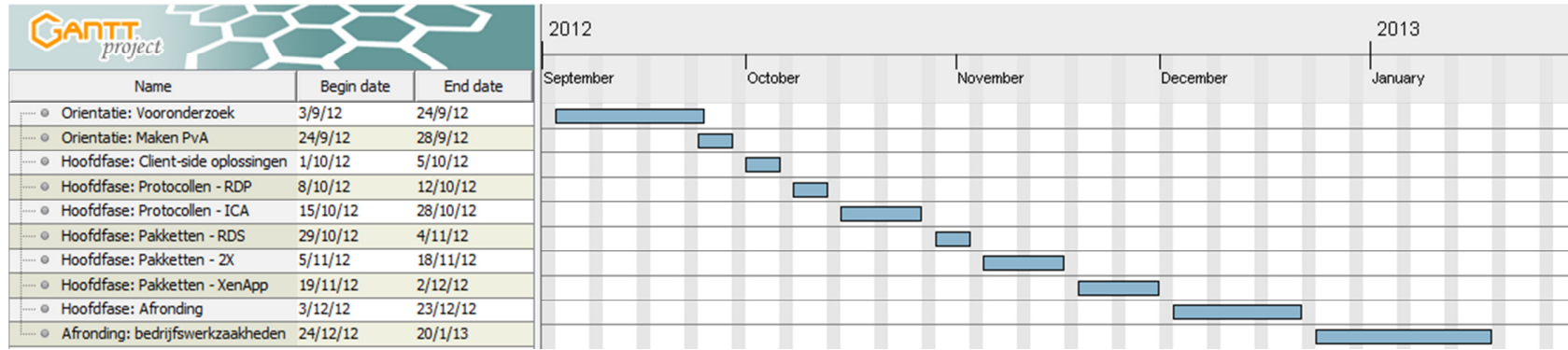
6.2 Planning:

6.2.1 Tabel:

36	03-09-12 t/m	Analyse en documentatie van de huidige situatie (resultaten opnemen in plan van aanpak)
37	10-09-12 t/m	<ul style="list-style-type: none"> - Algemeen onderzoek naar een verbeterde infrastructuur - Specifiek onderzoek naar Citrix en 2X en/of eventuele andere
38	17-09-12 t/m	<ul style="list-style-type: none"> - Algemeen onderzoek naar een verbeterde infrastructuur - Specifiek onderzoek naar zero clients (resultaten opnemen in plan
39	24-09-12 t/m	Onderzoek naar nieuwe manieren om de kinderwerkplek te ontsluiten, evt. cloud computing (resultaten opnemen in plan van aanpak)
39	24-09-12 t/m	Plan van aanpak af gaan ronden (uiterste inleverdatum 19-10-12).
40	01-10-12 t/m	Onderzoek naar client-side oplossingen
41	08-10-12 t/m	Onderzoek naar protocollen: RDP
42	15-10-12 t/m	Onderzoek naar protocollen: ICA
43	22-10-12 t/m	Onderzoek naar protocollen: ICA
44	29-10-12 t/m	Onderzoek naar pakketten: RDS
45	05-11-12 t/m	Onderrzoek naar Paketten: 2X
46	12-11-12 t/m 18-11-12	Onderrzoek naar Paketten: 2X

47	19-11-12 t/m	Onderrzoek naar Paketten: Citrix XenApp
48	26-11-12 t/m	Onderrzoek naar Paketten: Citrix XenApp
49 t/m 51	3-12-12 t/m 23-12-12	<ul style="list-style-type: none"> - Afronden van het hoofdonderzoek - Afronden adviesrapport - Proof of concept - schrijven scriptie (+-20 dagen zijn hiervoor gereserveerd), uiterlijk 18-12-12 inleveren.
52 t/m 3	24-12-12 t/m	Uitlooptijd: afronden van werkzaamheden op het bedrijf
1 t/m 5	01-01-13 t/m	Afstudeerzitting; precieze datum nog vast te stellen

6.2.2 Gantt chart:



6. Projectomgeving:

7.1 Partijen:

- Afstudeerder:

Naam: Daan de Boer
E-mail: daandeboer@gmail.com
Tel: 0652056744

- Bedrijfsbegeleider:

Naam: Marco van Thiel
E-mail: mvt@kinderwerkplek.nl
Tel: 0654211659

- Schoolbegeleider:

Naam: Petra Belgraver
E-mail: petra.belgraver@hu.nl
Tel: 0645061025

Bijlage 1: analyse van de eisen

B1.2: Aanvangssituatie, ontwerpdoelen en scope:

B1.2.1 Aanvangssituatie

Kinderwerkplek heeft op dit moment een werkende infrastructuur voor het aanbieden van kinderwerkplekken; deze voldoet echter niet aan de eisen voor multimedia en is niet schaalbaar genoeg.

Dat betekent dat de beginsituatie gekenschetst kan worden met **'Bestaand netwerk'**.

Het type van dit project is: **'Aanpassingen aan bestaande infrastructuur'**.

Het uiteindelijke doel is: **'Het opleveren van een schaalbare infrastructuur met kwaliteit multimedia ondersteuning.'**

Samenvattend: Het doel van dit project is het opstellen van een ontwerp voor een schaalbare infrastructuur. Dit omvat de infrastructuur in het datacenter alsmede de clients bij de klant. De bouw wordt aan anderen overgelaten. De werking van het opgeleverde ontwerp zal worden getest en gepresenteerd aan de hand van een Proof of Concept van de gewenste infrastructuur.

B1.2.2 Beperkingen

- Er bestaan beperkingen betreffende bestaande applicaties, computersystemen en netwerken. De performance van deze componenten mag niet noemenswaardig te lijden hebben onder de hogere kwaliteit multimedia (d.w.z. het verhoogde bandbreedte verbruik).
- De clients bij de klant zullen gekoppeld worden aan de infrastructuur van Kinderwerkplek via het internet. Als beperking geldt dat alleen vanuit de klant verbinding gemaakt mag worden met kinderwerkplek desktops.

B1.2.3 Scope

Binnen de scope van het project vallen:

- Advies m.b.t. een schaalbare infrastructuur die kwaliteit multimedia ondersteund
- Advies m.b.t. mogelijk te gebruiken protocollen
- Advies over mogelijk te gebruiken pakketten
- Vergelijkende proof of concepts
- Prijskwaliteitsvergelijkingsmatrix
- Implementatieplannen voor de levensvatbare oplossingen
- Advies m.b.t. alternatieve mogelijkheden om de kinderwerkplek aan te bieden (op mobile devices bijvoorbeeld, of vanuit de cloud)

Buiten de scope van het project vallen:

- Daadwerkelijke implementatie
- Advies m.b.t. het aanbieden van complete virtuele machines aan gebruikers (VDI)

B1.3: Locatie-informatie en plaatsing van computersystemen

B.1.3.1 Locaties

Reeds bij aanvang van het project stond vast dat er twee locaties zijn, waarop computersystemen geplaatst zijn en worden; het aantal client locaties zal stijgen naarmate er meer kinderwerkplekken verkocht worden:

- Routeit datacenter (servers)
- T-IC Utrecht (clients)

B.1.3.2 Computersystemen

In de infrastructuur zijn de volgende computersystemen opgenomen:

- Routeit bladeserver als virtual host voor de verschillende servers
 - Kinderwerkplek domain controller (server 2008 R2)
 - RDS session broker (server 2008 R2)
 - RDS session host (server 2008 R2)
- Bij de klant staan clients die verbinding maken met de RDS servers:
 - HP t5570 thin clients, ingebouwd in de kinderwerkplek meubels

B1.3: Gedragsskarakteristieken

B.1.3.1 Gebruikers

Als gebruikers van de infrastructuur van Kinderwerkplek kunnen we drie typen onderscheiden:

- De leerling binnen schooltijd speelt educatieve software, gebruikt office en doet onderzoek op internet;
- De buitenschoolse leerling speelt (flash) spelletjes en kijkt (flash) filmpjes;
- De leraren vragen eventuele nieuwe software en features aan.

B.1.3.2 Applicaties

We kunnen globaal vier applicatie “clusters” onderscheiden, te weten: session broker, session hosts, domain services en client OS. Deze applicaties zijn verantwoordelijk voor de volgende taken:

- Session broker
 - Bijhouden van logins en user informatie tussen sessies
 - Distribueren van de server load
- Session hosts:
 - Aanbieden van desktops
 - Aanbieden van applicaties
- Domain services
 - Authenticatie
 - Groep specifieke filtering
 - Groep specifiek applicatie aanbod
- Client OS:
 - (automatisch) verbinding maken met de servers

B1.3: Eisen:

Aan de hand van het onderstaande template zullen de eisen worden verzameld. De eisen zullen worden geselecteerd en ingedeeld aan de hand van de volgende criteria:

- Kerneisen, absoluut aan te voldoen voor het functioneren van het netwerk;
- Informatie-eisen, nodig om informatie over het functioneren van het netwerk te verkrijgen;
- Features, eisen die nuttig en prettig zijn, maar niet noodzakelijk voor het functioneren;
- Toekomstige eisen, die nuttig zijn in verband met upgrades en revisies;
- Afgewezen eisen, niet nuttige en overbodige eisen.

Het type eis kan Gebruiker (User), Applicatie (App), Host, Netwerk (Netw) of meta⁷⁴ zijn. Voor de uitleg van deze indeling zie de methode iAA&D.

Template:

Elke globale eis zal een uniek hoofdnummer krijgen (**10, 20, enz**); elke daarvan afgeleide eis krijgt een gesubordineerd nummer onder de eis waaruit hij is afgeleid (**11, 12, 21 enz.**).

⁷⁴ Meta in die zin, dat het niet om gewenste resultaten *van* het project gaat, maar om eisen m.b.t. het project zelf.

11	User	Internetfilter	Afhankelijk van de groep van het kind moeten	Klant	Kern	1
12	User	Internetfilter	Er moet een balans gevonden worden tussen	Klant	Kern	2
13	User	Internetfilter	Aanvankelijk moet veiligheid de meest nadruk krijgen; d.m.v. kinder- en leraren feedback wordt de	Klant	Kern	1
14	User	Internetfilter	Op aanvraag moeten bepaalde (combinaties) van termen en specifieke sites toegelaten kunnen	Klant	Kern	2
15		Internetfilter	Chatten op internet moet beveiligd kunnen worden	Klant	Kern	2
16		Internetfilter	Op verschillende tijdstippen moeten er andere filters	Klant	Kern	1
17		Internetfilter	De filter moet met tijdsquota kunne werken	Klant	Kern	2
18	Ann	Internetfilter	De filter moet active directory geïntegreerd zijn	Datacent	Feature	1
20	User	Applicatie aanbod	Afhankelijk van groep moeten verschillende	Klant	Kern	2
21	App	Applicatie aanbod	AD geïntegreerd	Datacent	Feature	1
22	User	Applicatie aanbod	Applicaties moeten touch-screen ondersteunen	Klant	Feature	3
30	Host	Responsiviteit	De dekstops moeten responsief blijven, zelfs bij	Klant	Kern	1
31	Host	Responsiviteit	De desktops mogen niet meer dan 300ms vertraging	Klant	Kern	1
32	Host	Responsiviteit	De desktops moeten indien mogelijk onder de	Klant	Feature	2
33	Host	Responsiviteit	Audio-video asynchroniciteit mag niet boven de	Klant	Kern	1
34	Netw.	Responsiviteit	Quality of service moet gebruikt kunnen worden om	Datacent	Kern	1
40	Netw.	Schaalbaarheid	De infrastructuur moet schaalbaar zijn	Datacent er	Kern	1
41	Netw.	Schaalbaarheid	Applicaties moeten on the fly toegevoegd kunnen worden	Datacent er	Kern	1
42	Netw.	Schaalbaarheid	Storage moet kunnen worden uitgebreid zonder onderliggende architectuur te veranderen	Datacent er	Kern	1
43	Netw.	Schaalbaarheid	De server farm moet kunnen worden uitgebreid zonder onderliggende architectuur te veranderen	Datacent er	Kern	1
44	Netw.	Schaalbaarheid	Load-balancing d.m.v. policies moet mogelijk zijn	Datacent er	Kern	1
45	Netw.	Schaalbaarheid	Aanbieden van complete virtuele desktops (VDI)	Klant	Afgewezen	-
46	Netw.	Schaalbaarheid	Multimedia- en flash redirectie moet mogelijk zijn	Datacent	Kern	1
48	Netw.	Schaalbaarheid	Clients moeten d.m.v. redirectie last van de servers	Klant	Feature	2

Bijlage 2: Zelfevaluatie:

In overleg met mijn bedrijfsbegeleider (Marco van Thiel) en collega's had ik al vrij snel een idee van wat ik wilde gaan onderzoeken. Ik vond het echter lastig hier op een gestructureerde manier aan te beginnen. Dankzij het regelmatige overleg met Petra Belgraver (mijn begeleider vanuit school) heb uiteindelijk in mijn plan van aanpak een concrete en gestructureerde lijst met eisen gemaakt, die zeer geschikt was om het onderzoek in goede banen te leiden. Dit heeft me erg geholpen gedurende het hele project.

Vanaf dat moment ging het snel. Ik heb veel technisch onderzoek gedaan en de resultaten opgenomen in mijn scriptie. Daarnaast heb ik twee proof of concepts gemaakt (één voor elk pakket), die beide werkend gedraaid hebben. Deze hebben erg geholpen bij het maken van het uiteindelijke advies.

Tegen het einde van de periode werd het echter nog lastig. Ik had iets meer als 20 dagen ingepland om mijn scriptie te schrijven (het aantal aangeraden door school). Op het moment dat ik er aan wilde beginnen deed zich echter een probleem voor. Een migratie van een telefooncentrale die gepland stond als één maand durend project, werd vooruitgeschoven vanwege een calamiteit met de huidige telefooncentrale. Het project moest nu in de helft van de geplande tijd uitgevoerd worden.

Het was alle hands aan dek dus. Ik heb vrijwel de gehele periode meegewerkt aan dit project. Ik heb zoveel mogelijk tussendoor en 's avonds aan mijn scriptie gewerkt, maar ben in totaal toch zo'n tien dagen kwijtgeraakt. Hierdoor heb ik mijn scriptie niet op tijd af kunnen krijgen, en moest deze dus met uitstel ingeleverd worden. Daarnaast was mijn scriptie op een gegeven moment zeer chaotisch en fragmentarisch, omdat ik zoveel tussen de bedrijven door gewerkt had. Dit heb ik uiteindelijk kunnen herstellen tijdens een week thuiswerken na de migratie (tijdens de uitstelperiode).

Een lastig begin en einde dus, maar ik heb er veel van geleerd. Vooral het plan van aanpak (en de hulp van Petra Belgraver daarbij) heeft me veel geleerd over het gestructureerd beginnen van een project: het concreet maken van de eisen, planning, doelstelling, enz.

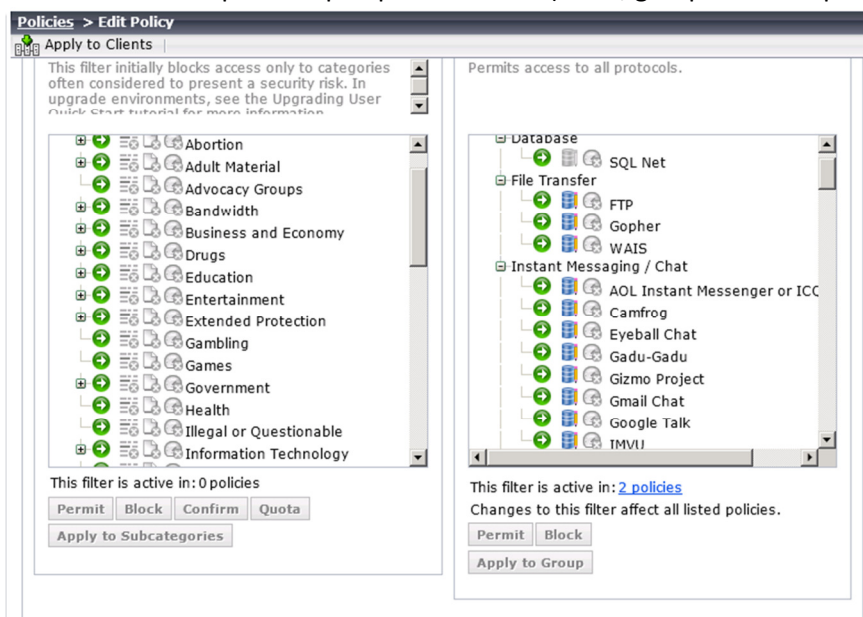
En hoewel ik—dit op de laatste dag schrijvende—nog steeds veel zaken zie die ik nog zou willen verbeteren (een nooit ophoudend proces bij mij), ben ik toch tevreden met het werk dat ik geleverd heb en de vele dingen die ik heb geleerd.

Bijlage 3: Webfilters:

Eisen Websense:

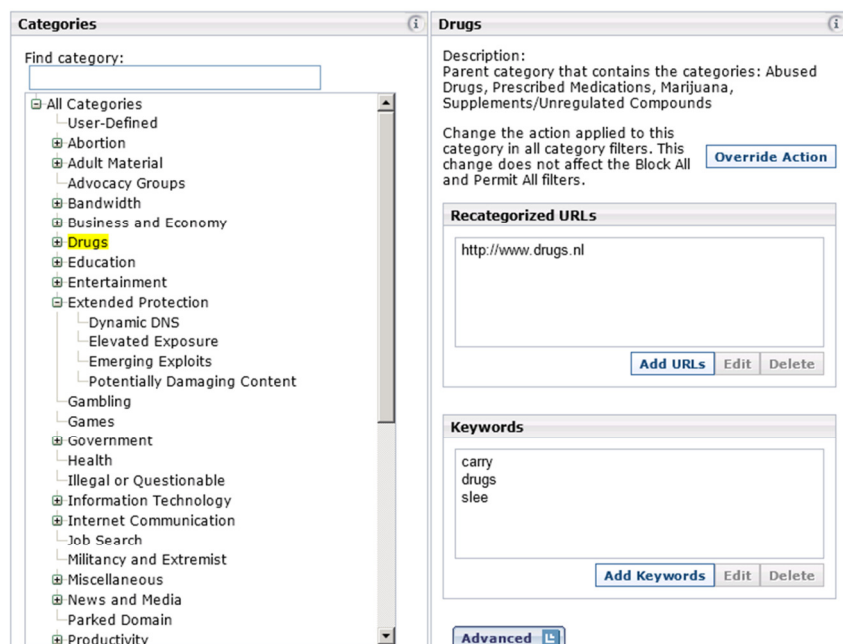
Afhankelijk van de groep van het kind moeten verschillende onderwerpen gefilterd worden

Dit is mogelijk; bepaalde categoriën kunnen toegelaten of geblokkeerd worden, vervolgens kan gekozen worden dit toe te passen op bepaalde clients (users, groepen of computers)



Op aanvraag moeten bepaalde (combinaties) van termen en specifieke sites toegelaten kunnen worden.

Dit is beperkt mogelijk; sites en termen kunnen toegelaten worden, maar geen combinaties van termen. Dit is lastig als je bijvoorbeeld wel drugs wilt blokkeren, maar niet carrie slee *en* drugs; dit is

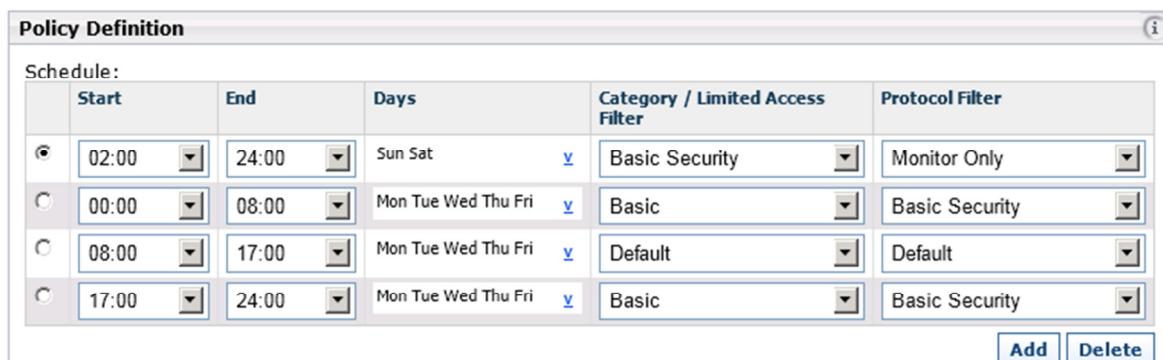


Chatten op internet moet beveiligd kunnen worden:

Chatsites en chat protocollen kunnen gefilterd worden; er kan echter geen standaard waarschuwing gegeven worden in de chatprogramma's zelf, die de personen waar de kinderen mee chatten waarschuwt dat ze gemonitord worden.

Op verschillende tijdstippen moeten er andere filters kunnen gelden

Dit is mogelijk.



Policy Definition					
Schedule:					
	Start	End	Days	Category / Limited Access Filter	Protocol Filter
<input checked="" type="radio"/>	02:00	24:00	Sun Sat	Basic Security	Monitor Only
<input type="radio"/>	00:00	08:00	Mon Tue Wed Thu Fri	Basic	Basic Security
<input type="radio"/>	08:00	17:00	Mon Tue Wed Thu Fri	Default	Default
<input type="radio"/>	17:00	24:00	Mon Tue Wed Thu Fri	Basic	Basic Security

Add Delete

De filter moet met tijdsquota kunne werken

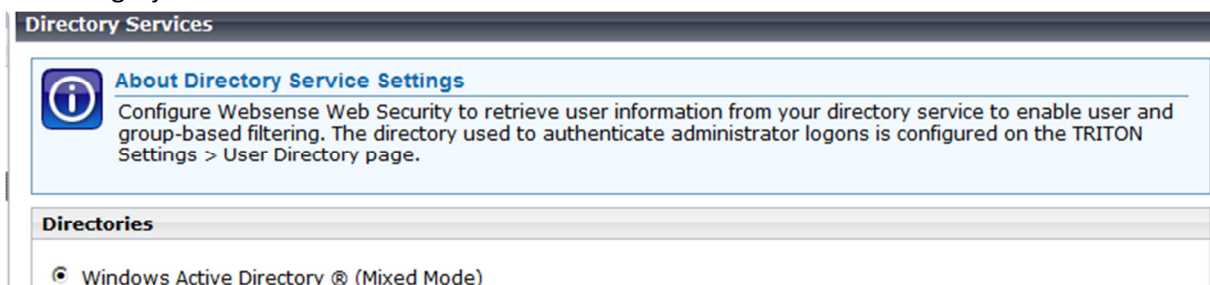
Quota session length: minutes

Default quota time per day: minutes

Default quota sessions per day: 6

De filter moet active directory geïntegreerd zijn.

Dit is mogelijk:



Directory Services

About Directory Service Settings
 Configure Websense Web Security to retrieve user information from your directory service to enable user and group-based filtering. The directory used to authenticate administrator logons is configured on the TRITON Settings > User Directory page.

Directories

- ☒ Windows Active Directory ® (Mixed Mode)

Eisen Yoursafetynet:

Afhankelijk van de groep van het kind moeten verschillende onderwerpen gefilterd worden

Dit is mogelijk; bepaalde categoriën kunnen toegelaten of geblokkeerd worden, vervolgens kan gekozen worden dit toe te passen op bepaalde clients (users, groepen of computers)



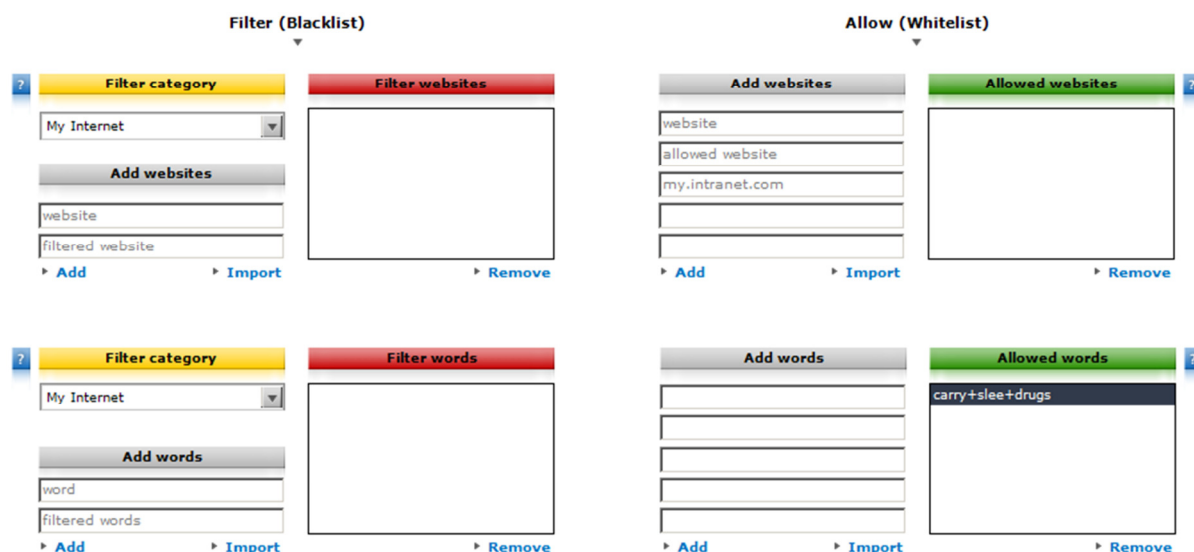
The interface is divided into two main sections: '1. Users' and '2. Filters'.

1. Users: A table with a header 'Users' and two rows of users: 'daan (Admin)' and 'test'. Both rows have a checked checkbox in the first column.

2. Filters: Two columns of filter categories. The 'Internet' column has a yellow header and lists: Drugs, Gambling, Pro-Ana, Sex, Weapons, and My Internet, each with a green circle icon. The 'Media' column has a green header and lists: Chat, Games-Offline, Games-Online, Internet Phone, Peer-to-Peer, Social Networks, and My Media, each with a red circle icon.

Op aanvraag moeten bepaalde (combinaties) van termen en specifieke sites toegelaten kunnen worden.

Dit is mogelijk; sites en (combinaties van) termen kunnen toegelaten worden, zoals rechtsonderin onderstaand figuur te zien. Dit is ook als werkend getest; drugs werd geblokkeerd, carry see + drugs



The interface is divided into two main sections: 'Filter (Blacklist)' and 'Allow (Whitelist)'.

Filter (Blacklist): This section contains two sub-panels. The top panel is for 'Filter websites' and the bottom panel is for 'Filter words'. Both panels have a 'Filter category' dropdown set to 'My Internet', an 'Add' button, and an 'Import' button. The 'Filter websites' panel has a 'Filter websites' table with one row: 'website'. The 'Filter words' panel has a 'Filter words' table with one row: 'word'.

Allow (Whitelist): This section contains two sub-panels. The top panel is for 'Allowed websites' and the bottom panel is for 'Allowed words'. Both panels have an 'Add' button, an 'Import' button, and a 'Remove' button. The 'Allowed websites' panel has an 'Add websites' table with three rows: 'website', 'allowed website', and 'my.intranet.com'. The 'Allowed words' panel has an 'Add words' table with one row: 'carry+slee+drugs'.

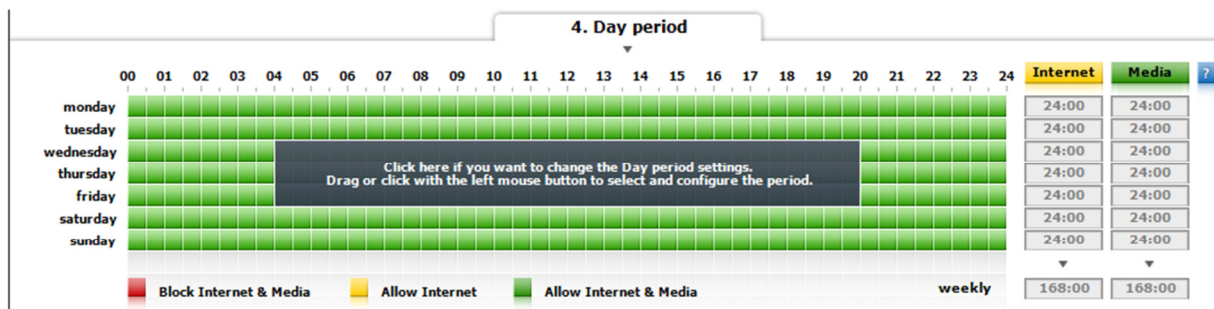
Chatten op internet moet beveiligd kunnen worden:

Dit is mogelijk; er kan bij het chatten standaard een waarschuwing gegeven worden aan de persoon waar de kinderen mee chatten:



Op verschillende tijdstippen moeten er andere filters kunnen gelden

Dit is mogelijk:



De filter moet met tijdsquota kunne werken

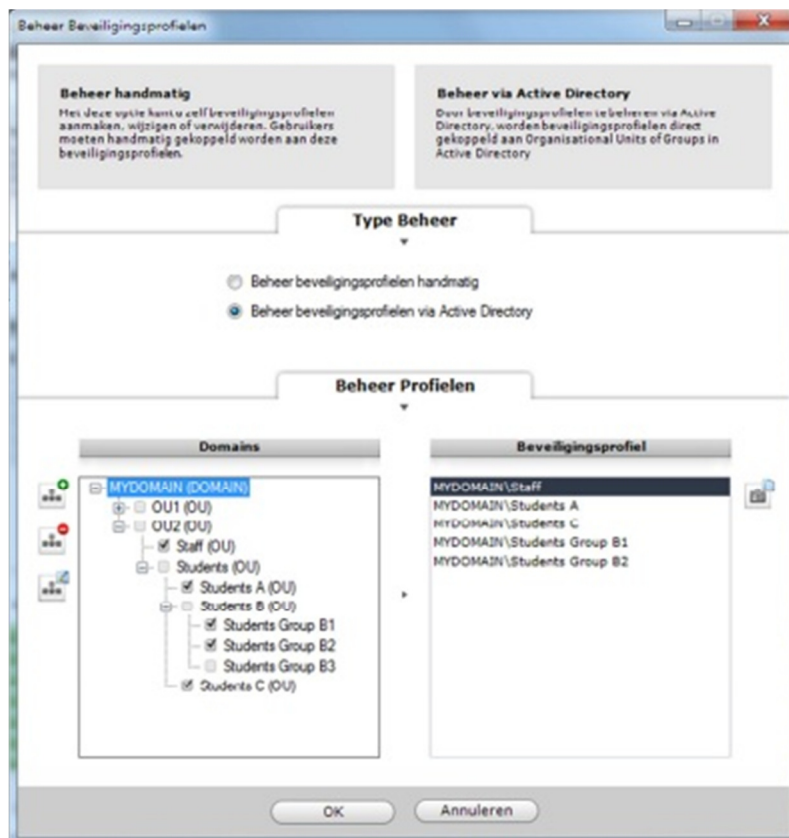
3. Day limits

Internet Media ?

monday	24:00	24:00
tuesday	24:00	24:00
wednesday	24:00	24:00
thursday	24:00	24:00
friday	24:00	24:00
saturday	24:00	24:00
sunday	24:00	24:00
weekly	168:00	168:00

De filter moet active directory geïntegreerd zijn.

Dit is mogelijk:



Bijlage 4: Proof of concept:

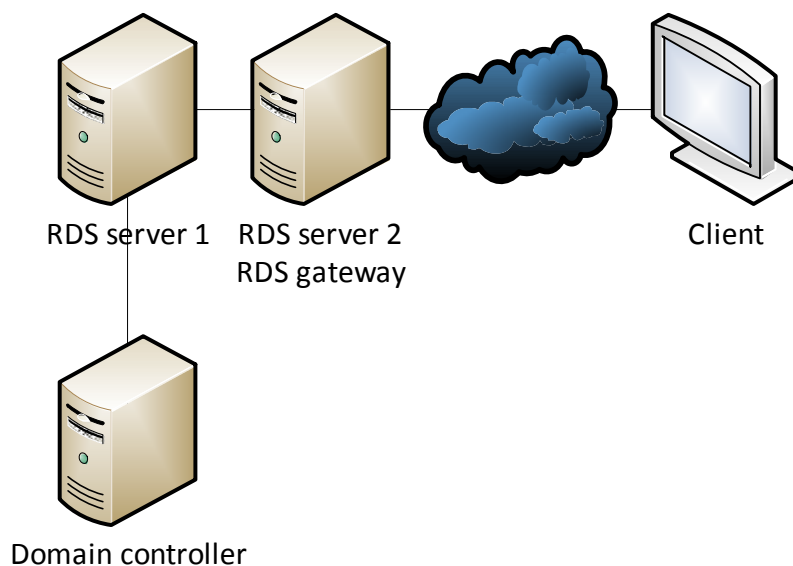
Proof of concept

Het proof of concept (vanaf nu PoC) is opgezet om te demonstreren dat de opzet uit het advies ook daadwerkelijk kan werken. In het PoC zijn twee zaken getest: of de pakketten aan de functionele eisen voldoen, en de performance en het resource verbruik van de oplossingen.

Voor beide pakketten is een opstelling gemaakt. Hieronder wordt voor zowel RDS als XenApp eerst de opstelling uiteengezet en vervolgens worden de resultaten kort samengevat:

RDS:

Opstelling:



Onderdeel: Hardware:

RDS server 1 Proliant ML110 G6 (Xeon X3430@2.4GHz CPU met 8GB memory)

RDS server 2 Proliant ML110 G6 (Xeon X3430@2.4GHz CPU met 8GB memory)

Domain controller HP Proliant ML110 G6 (Xeon X3430@2.4GHz CPU met 8GB memory)

Client MSI Notebook CX70-0ND (Intel Core i5 3210M@2.5GHz CPU met 8GB memory)

In deze opzet worden twee RDS servers gebruikt; deze zijn allebei session-hosts. De tweede server is tevens ook gateway en zorgt voor externe toegang tot de desktops. De domain controller zorgt voor authenticatie.

De client zal verbinding maken en een desktop gebruiken om de oplossing te testen.

Resultaten:

Eisen:

De eisen die in de scriptie naar voren kwamen zijn getest in het PoC. Hierbij is het volgende geconcludeerd:

20	Applicatie aanbod	Afhankelijk van groep moeten verschillende	2	Ja
31	Responsiviteit	De desktops mogen niet meer dan 300ms vertraging	1	Ja
32	Responsiviteit	De desktops moeten indien mogelijk onder de	2	Ja
33	Responsiviteit	Audio-video asynchroniciteit mag niet boven de	1	Ja
34	Responsiviteit	Quality of service moet gebruikt kunnen worden om	1	Nee
41	Schaalbaarheid	Applicaties moeten on the fly toegevoegd kunnen	1	Ja
43	Schaalbaarheid	De server farm moet kunnen worden uitgebreid	1	Ja
44	Schaalbaarheid	Load-balancing d.m.v. policies moet mogelijk zijn	1	Nee
46	Schaalbaarheid	Multimedia- en flash redirectie moet mogelijk zijn	1	Ja
48	Schaalbaarheid	Clients moeten d.m.v. redirectie last van de servers	2	Nee ⁷⁵

⁷⁵ In wat volgt zal blijken waarom hier niet aan voldaan wordt.

Performance:

Om de performance te testen heeft de client verbinding gemaakt met de server om een desktop te krijgen; vervolgens is op de desktop een HD filmpje op youtube afgespeeld. Het betreft het filmpje “How big is the universe: HD”⁷⁶. Deze is gekozen omdat het zowel rustige stukken heeft (enkel het zwart van de ruimte) als veeleisende stukken (duizenden sterren, waardoor erg veel grafische data verwerkt moet worden). Het filmpje is veel zwaarder dan wat doorgaans afgespeeld zal worden; hier is voor gekozen omdat het de verschillen tussen de pakketten het beste naar voren zal brengen door ze te overdrijven. Deze tests zijn ook opgenomen op video⁷⁷.

Het afspelen van deze video kostte bij RDS gemiddeld zo’n 60% CPU (het gaat om de bovenste vier processen); op de client werd ongeveer 10% CPU verbruikt (vanwege flash redirection):

⁷⁶ <http://www.youtube.com/watch?v=JvdL3R7fDL4>

⁷⁷ Zie: <http://www.youtube.com/user/ddb1574031?feature=mhee>

naam	Status	CPU	Memory
Google Chrome (32 bit)		47.0%	88.8 MB
> Google Chrome (32 bit)		7.2%	33.8 MB
Google Chrome (32 bit)		2.9%	98.6 MB
> termsvcs		2.0%	65.8 MB
Desktop Window Manager		1.0%	8.4 MB
Google Chrome (32 bit)		0.7%	47.3 MB
System		0.1%	0.1 MB
System interrupts		0%	0 MB
Client Server Runtime Process		0%	1.3 MB
> Service Host: DCOM Server Proc...		0%	2.1 MB
> Task Manager		0%	7.4 MB
> SQL Server Windows NT - 64 Bit		0%	56.7 MB
Windows Explorer		0%	9.4 MB
RDP Clipboard Monitor		0%	1.3 MB
> Service Host: Local System (13)		0%	15.3 MB
> Service Host: Local Service (Net...		0%	7.6 MB
> Service Host: Remote Procedure...		0%	2.0 MB
> Service Host: Network Service (5)		0%	5.6 MB
> Service Host: Local System (Net...		0%	3.4 MB
> Local Security Authority Process...		0%	3.8 MB

the universe hd

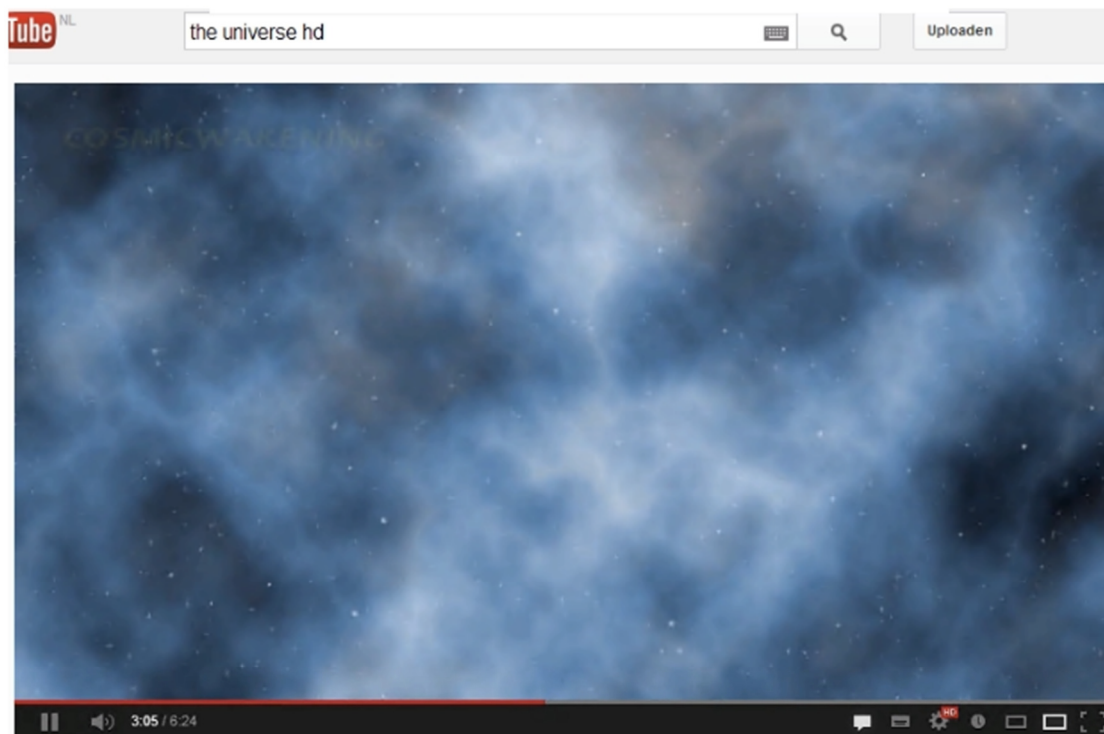


Uploaden



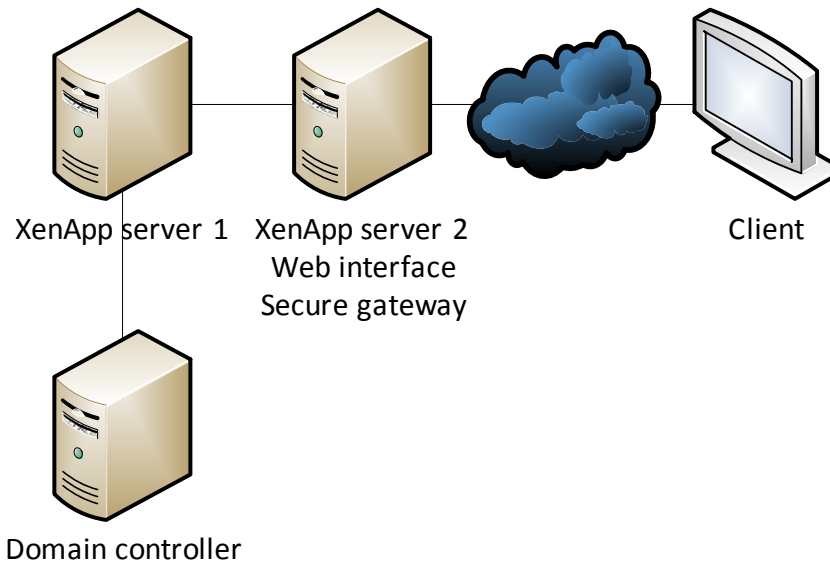
Er werden echter pieken van 80% gehaald bij intensieve stukken:

Processes			
Performance Users Details Services			
Name	Status	80% CPU	17% Memory
Google Chrome (32 bit)		49.6%	88.8 MB
Google Chrome (32 bit)		14.8%	98.8 MB
termsvcs		10.4%	65.8 MB
Google Chrome (32 bit)		3.7%	33.8 MB
Desktop Window Manager		1.3%	8.4 MB
Google Chrome (32 bit)		0.6%	47.3 MB
System		0.1%	0.1 MB
System interrupts		0%	0 MB
SQL Server Windows NT - 64 Bit		0%	51.2 MB
Client Server Runtime Process		0%	1.3 MB
Service Host: DCOM Server Proc...		0%	2.1 MB
Task Manager		0%	7.4 MB
Windows Explorer		0%	9.4 MB
RDP Clipboard Monitor		0%	1.3 MB
Service Host: Local System (13)		0%	15.3 MB
Service Host: Local Service (Net...		0%	7.6 MB
Service Host: Remote Procedure...		0%	2.0 MB
Service Host: Network Service (5)		0%	5.6 MB
Service Host: Local System (Net...		0%	3.4 MB
Local Security Authority Process...		0%	3.7 MB
Services and Controller app		0%	2.8 MB



Citrix XenApp:

Opstelling:



In deze opzet worden twee XenApp servers gebruikt; deze zijn allebei session-hosts. De tweede server zorgt voor externe toegang tot de desktops d.m.v. web interface en Secure Gateway. De domain controller zorgt voor authenticatie.

De client zal verbinding maken en een desktop gebruiken om de oplossing te testen.

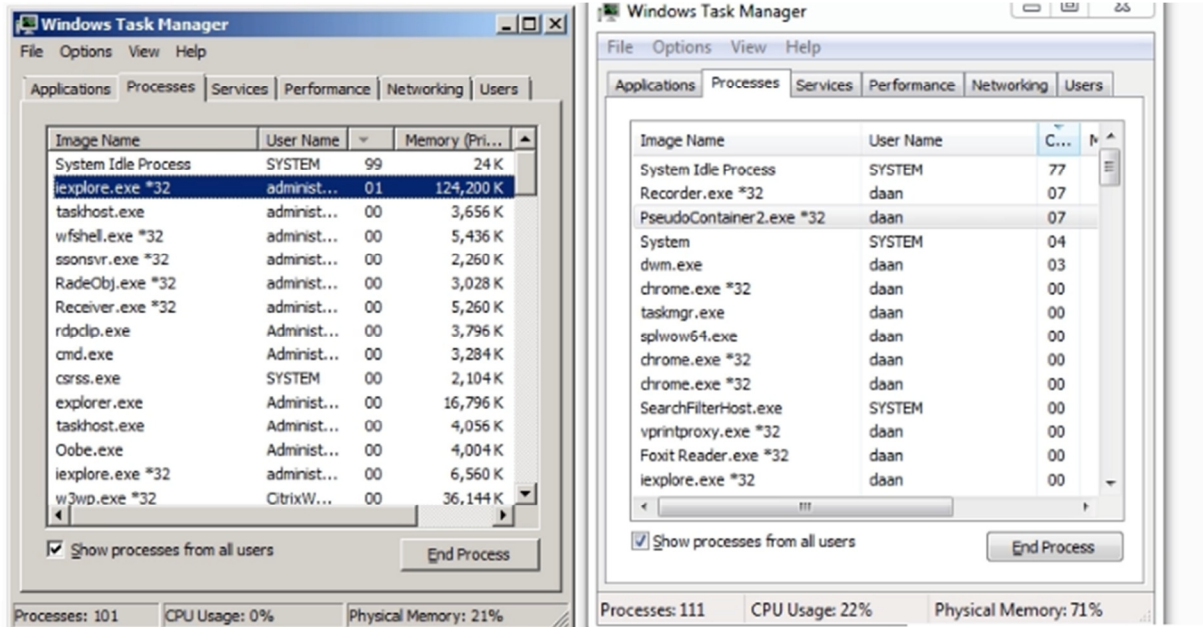
Resultaten:

Eisen:

20	Applicatie aanbod	Afhankelijk van groep moeten verschillende	2	Ja
31	Responsiviteit	De desktops mogen niet meer dan 300ms vertraging	1	Ja
32	Responsiviteit	De desktops moeten indien mogelijk onder de	2	Ja
33	Responsiviteit	Audio-video asynchroniteit mag niet boven de	1	Ja
34	Responsiviteit	Quality of service moet gebruikt kunnen worden om	1	Ja
41	Schaalbaarheid	Applicaties moeten on the fly toegevoegd kunnen	1	Ja
43	Schaalbaarheid	De server farm moet kunnen worden uitgebreid	1	Ja
44	Schaalbaarheid	Load-balancing d.m.v. policies moet mogelijk zijn	1	Ja
46	Schaalbaarheid	Multimedia- en flash redirectie moet mogelijk zijn	1	Ja
48	Schaalbaarheid	Clients moeten d.m.v. redirectie last van de servers	2	Ja

Performance:

Het gemiddelde CPU gebruik op de server is 0%. Op de client wordt 3 tot 7% (5% gemiddeld) CPU verbruikt.



Intensievere stukken lijken geen indruk te maken op XenApp: het verbruik is 3% op de client:

Windows Task Manager

Image Name	User Name	Memory (Pri...)
System Idle Process	SYSTEM	24 K
taskhost.exe	administ...	3,656 K
wfshell.exe *32	administ...	5,436 K
ssonsvr.exe *32	administ...	2,260 K
RadeObj.exe *32	administ...	3,028 K
Receiver.exe *32	administ...	5,260 K
rdpdp.exe	Administ...	3,796 K
cmd.exe	Administ...	3,284 K
csrss.exe	SYSTEM	2,104 K
explorer.exe	Administ...	16,796 K
taskhost.exe	Administ...	4,056 K
Oobe.exe	Administ...	3,752 K
iexplore.exe *32	administ...	6,560 K
w3wp.exe *32	CitrixW...	36,152 K
dwm.exe	administ...	3,456 K

Processes: 101 CPU Usage: 0% Physical Memory: 21%

Windows Task Manager

Image Name	User Name	C...
System Idle Process	SYSTEM	87
Recorder.exe *32	daan	05
PseudoContainer2.exe *32	daan	03
dwm.exe	daan	02
System	SYSTEM	01
chrome.exe *32	daan	00
taskmgr.exe	daan	00
splwow64.exe	daan	00
chrome.exe *32	daan	00
chrome.exe *32	daan	00
vprintproxy.exe *32	daan	00
Foxit Reader.exe *32	daan	00
iexplore.exe *32	daan	00
vmware.exe *32	daan	00

Processes: 109 CPU Usage: 12% Physical Memory: 71%





Conclusie:

Hoewel RDS flash redirectie gebruikt, wordt er toch zéér veel CPU kracht verbruikt. De reden hiervoor is reeds in het onderzoek naar voren gekomen: RDS identificeert de video elementen in de remote desktop sessie en gebruikt compressie op deze elementen; vervolgens stuurt hij ze naar de client die ze weer uitpakt. Hierdoor moeten zowel de server als de client werkt verrichten. Vooral de server heeft het zwaar te verduren, zo bleek uit de test. Aangezien het hele punt van flash redirectie is om de server load te verminderen, komt RDS niet goed naar voren in deze test.

XenApp daarentegen gebruikt géén server resources; het is ware flash redirectie. Al het werk wordt door de client gedaan. Het is noemenswaardig dat ondanks dit feit de client met XenApp alsnog minder te doen heeft dan met RDS (5% tegen 10% respectievelijk).

Niet alleen voldoet XenApp aan meer eisen dan RDS (aan alle eisen zelfs), het verbruikt ook minder resources op de server.

Biilage 5: Vergelijkingsmatrix:

Vergelijkingsmatrix				
ID:	Eis:	Prio:	Wordt er aan de eis voldaan?	
20	Afhankelijk van groep moeten verschillende applicaties aangeboden worden	2	Ja	Ja
21	AD geïntegreerd	1	Ja	Ja
22	Applicaties moeten touch-screen ondersteunen	3	Ja	Ja
31	De desktops mogen niet meer dan 300ms vertraging hebben	1	Ja	Ja
32	De desktops moeten indien mogelijk onder de 150ms vertraging blijven	2	Ja	Ja
47	Quality of service moet gebruikt kunnen worden om interactieve data voorrang te geven	1	Nee	Ja
33	Audio-video asynchroniciteit mag niet boven de 22ms komen	1	Ja	Ja
41	Applicaties moeten on the fly toegevoegd kunnen worden	1	Ja	Ja
42	Storage moet kunnen worden uitgebreid zonder onderliggende architectuur te veranderen	1	Ja	Ja
43	De server farm moet kunnen worden uitgebreid zonder onderliggende architectuur te veranderen	1	Ja	Ja
44	Load-balancing d.m.v. policies moet mogelijk zijn	1	Nee	Ja
46	Multimedia- en flash redirectie moet mogelijk zijn	1	Gedeeltelijk	Ja

Totaalpunten applicatie eisen:
Totaalpunten responsiviteit eisen:
Totaalpunten schaalbaarheid eisen:
Totaal:

Uitleg:

De pakketten worden d.m.v. punten beoordeeld. Per eis kunnen er punten verdiend worden; hoeveel punten dit zijn hangt af van twee zaken: of er aan de eis vo
Als er aan een eis voldaan wordt, krijgt het pakket 4 punten voor een prio 1 eis; 3 punten voor een prio 2 eis, en 2 punten voor een prio 3 eis. Als er gedeeltelijk aa
Als een pakket niet aan een eis voldoet krijg het 0 punten.

